User Guide - English

FUJITSU

ServerView Suite

Remote Management

iRMC S2/S3 - integrated Remote Management Controller

Edition July 2012

Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to manuals@fujitsu-siemens.com.

Certified documentation according to DIN EN ISO 9001:2008

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2008.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright and Trademarks

Contents

1 Preface

Modern server systems are becoming increasingly complex. The requirements with respect to the management of such systems are growing accordingly.

In response to this development, a number of vendors founded the “Intelligent Platform Management Interface” (IPMI) initiative with the objective of defining a standardized, abstract, message-based interface between the central system controller (Baseboard Management Controller - BMC) and intelligent hardware for platform management. For further details on IPMI, please refer to section "IPMI - technical background" on page 21.

The **i**ntegrated **R**emote **M**anagement **C**ontrollers iRMC S2 and iRMC S3 (in the following iRMC S2/S3 for short) each represent a BMC with integrated LAN connection and extended functionality. In this way, the iRMC S2/S3 offers comprehensive control over PRIMERGY servers, irrespective of the system status. In particular, the iRMC S2/S3 allows for out-of-band management (Lights Out Management, LOM) of PRIMERGY servers. Out-of-band management uses of a dedicated management channel that enables a system administrator to monitor and manage servers via remote control regardless of whether the server is powered on.

Figure 1: iRMC S2 on the system board of a PRIMERGY server

As an autonomous system on the system board of a modern PRIMERGY server, the iRMC S2/S3 has its own operating system, its own web server, separate user management and independent alert management. The iRMC S2/S3 remains powered up even when the server is in stand-by mode.

This manual describes how to configure the iRMC S2/S3 and the various user interfaces available.

1.1 Purpose and target groups of the manual

This manual is aimed at system administrators, network administrators, and service staff who have a sound knowledge of hardware and software. It provides basic information on the technology behind IPMI and deals with the following aspects in detail:

- Logging on to the iRMC S2/S3
- Configuring the iRMC S2/S3
- User management on the iRMC S2/S3
- Advanced Video Redirection via iRMC S2/S3
- Remote Storage via iRMC S2/S3
- iRMC S2/S3 web interface
- Telnet/SSH-based interface (Remote Manager) of the iRMC S2/S3
- Configuring the iRMC S2/S3 with the Server Configuration Manager
- Updating the firmware
- Remote installation of the operating system via iRMC S2/S3
- IPMI OEM Commands

Service

If you have any further questions on remote management for PRIMERGY servers, contact the service and support partners responsible for you.

Other information

http://www.ts.fujitsu.com

1.2 Functions of the iRMC S2/S3 (overview)

The iRMC S2/S3 supports a wide range of functions that are provided by default. With Advanced Video Redirection (AVR) and Remote Storage, the iRMC S2/S3 also provides two additional advanced features for the remote management of PRIMERGY servers. To use AVR and Remote Storage, you require a valid license key, which can be purchased separately.

Standard functions of the iRMC S2/S3

- Browser access

  The iRMC S2/S3 features its own web server which can be accessed by the management station from a standard web browser.

- Security (SSL, SSH)

  Secure access to the Web server and secure graphical console redirection including mouse and keyboard can be provided over HTTPS/SSL. An encrypted connection protected using SSH mechanisms can be set up to access the iRMC S2/S3 using the Remote Manager. The Remote Manager is an alphanumeric user interface for the iRMC S2/S3.

- ServerView Integration

  The ServerView agents detect the iRMC S2/S3 and automatically assign it to the relevant server. This means that it is possible to start the iRMC S2/S3 web interface and text console redirection using the ServerView Remote Management Frontend directly from ServerView Operations Manager.

- Power management

  Irrespective of the status of the system, you have the following options for powering the managed server up or down from the remote workstation

  - using the iRMC S2/S3 web interface
  - using the Remote Manager and the command line interface (CLP)
  - with a script.

- Power consumption control

  The iRMC S2/S3 allows comprehensive power consumption control on the managed server. In addition, you can specify the mode (minimum power consumption or maximum performance) that the iRMC S2/S3 uses to control power consumption on the managed server. You can switch between these modes as required.

- Customer Self Service (CSS)

  Summary tables for the server components, sensors and the power supply on the iRMC S2/S3 web interface provide information in a separate column as to whether the server component affected is a CSS component or not. In addition, error list of the system event log (SEL) shows for every event whether it has been triggered by a CSS component.

- Text console redirection

  You can start a Telnet/SSH session to the iRMC S2/S3 from the ServerView Remote Management Frontend. This calls the Remote Manager, via which you can start a text console redirection session.

- Basic functions of a BMC

  The iRMC S2/S3 supports the basic functions of a BMC such as voltage monitoring, event logging and recovery control.

- “Headless” system operation

  The managed server does not require a mouse, monitor or keyboard to be connected. The benefits of this include lower costs, far simpler cabling in the rack and increased security.

- Identification LED

  To facilitate identification of the system, for instance if it is installed in a fully populated rack, you can activate the identification LED from the iRMC S2/S3 web interface.

- Global error LED

  A global error LED informs you of the status of the managed system at all times and at the same time shows the CSS (Customer Self Service) status.

- Power LED

  The power LED informs you whether the server is currently switched on or off.

- LAN

  On some systems, the LAN interface of the fitted system NIC (Network Interface Card) on the server is reserved for the management LAN. On other systems, you have the option of configuring this LAN interface to

  – reserve it for the management LAN
  – set it up for shared operation with the system or
  – make it completely available to the system.

  The ports marked with a wrench symbol are assigned to the iRMC S2/S3 (see figure 7 on page 42).

- Command line interface (CLP)

  In addition to the Remote Manager, the iRMC S2/S3 also supports SMASH CLP (**S**ystem **M**anagement **A**rchitecture for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol) as standardized by the DMTF (Distributed Management Task Force).

- Simple configuration - interactive or script-based

  The following tools are available for configuring the iRMC S2/S3:

  – iRMC web interface
  – Server Configuration Manager
  – The server management tool IPMIVIEW
  – BIOS Setup

  It is also possible to carry out configuration with the Server Configuration Manager or IPMIVIEW using scripts. This means that it is possible to configure the iRMC S2/S3 when the server is first configured via ServerView Installation Manager. It is also possible to configure a large number of servers on the basis of scripts.

- Support for the LocalView service panel

  If PRIMERGY servers are equipped with a ServerView local service panel, this module allows you to determine what module is faulty and whether you can replace the faulty module yourself.

- Local user management

  The iRMC S2/S3 has its own user management function which allows up to 16 users to be created with passwords and to be assigned various rights depending on the user groups they belong to.

- Global user management using a directory service

  The global user IDs for the iRMC S2/S3 are stored centrally in the directory service's directory. This makes it possible to manage the user identifications on a central server. They can therefore be used by all the iRMC S2/S3s that are connected to this server in the network.

  The following directory services are currently supported for iRMC S2/S3 user management:

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP
  – OpenDS

- CAS-based single sign-on (SSO) authentication

  The iRMC S2/S3 supports Centralized Authentication Service (CAS) configuration, which allows you to configure the iRMC S2/S3 web interface for CAS-based single sign-on (SSO) authentication.

  The first time a user logs in to an application (e.g. the iRMC S2/S3 web interface) within the SSO domain of the CAS service, they are prompted for their credentials by the CAS-specific login screen. Once they have been successfully authenticated by the CAS service, the user is granted access to the iRMC S2/S3 web interface as well as to any other service within the SSO domain without being prompted for login credentials again.

- DNS / DHCP

  The iRMC S2/S3 provides support for automatic network configuration. It has a default name and DHCP support is set by default so that the iRMC S2/S3 gets its IP address from the DHCP server. The iRMC S2/S3 name is registered by the Domain Name Service (DNS). Up to five DNS servers are supported. If DNS/DHCP is not available, the iRMC S2/S3 also supports static IP addresses.

- Power supply

  The iRMC S2/S3 is powered by the standby supply of the system.

- Alert management

  The alert management facility of the iRMC S2/S3 provides the following options for forwarding alerts (alerting):

  – Platform Event Traps (PET) are sent via SNMP.

  – Direct alerting by email.

  - A modem can be connected to the serial interface. This can then be used to send alerts (e.g. to a mobile phone via SMS).

  In addition, the iRMC S2/S3 provides the ServerView agents with all the relevant information.

- Read, filter and save the system event log (SEL).

  You can view, save and delete the contents of the SEL

  - by using the iRMC S2/S3 web interface or
  - by using the Telnet/SSH-based interface (Remote Manager) of the iRMC S2/S3.

- Read, filter and save the internal event log (iEL).

  You can view, save and delete the contents of the iEL

  - by using the iRMC S2/S3 web interface or
  - by using the Telnet/SSH-based interface (Remote Manager) of the iRMC S2/S3.

Extended functionality of the iRMC S2/S3

Alongside the standard functionality, the iRMC S2/S3 also supports the Advanced Video Redirection and Remote Storage functions.

- Advanced Video Redirection (AVR)

  The iRMC S2/S3 supports Advanced Video Redirection which offers the following benefits:

  - Operation over a standard web browser. No additional software needs to be installed in the management station other than the Java Runtime Environment.
  - System-independent graphical and text console redirection (including mouse and keyboard).
  - Remote access for boot monitoring, BIOS administration and operation of the operating system.
  - AVR supports up to two simultaneous “virtual connections” for working on a server from a different location. It also reduces the load on the network by using hardware and video compression.

- Local monitor-off support: It is possible to power down the local screen of the managed PRIMERGY server during an AVR session in order to prevent unauthorized persons from observing user input and actions carried out on the local server screen during the AVR session.
- Low bandwidth

  In the case of a reduced data transfer rate, you can configure a lower bandwidth (bits per pixel, bpp) in terms of color depth for your current AVR session.

- Remote Storage

  Remote Storage makes a “virtual” drive available which is physically located on a remote workstation or made available centrally on the network using a Remote Storage server.

  The “virtual” drives available with Remote Storage are simply managed in much the same way as local drives and offer the following options:

  - Read and write data.
  - Boot from Remote Storage.
  - Install drivers and small applications.
  - Update BIOS from remote workstation.
    (BIOS update via USB)

  Remote Storage supports the following device types to provide a “virtual drive” on the remote workstation:

  - CD ROM
  - DVD ROM
  - Memory stick
  - Floppy image
  - CD ISO image
  - DVD ISO image

  A Remote Storage server provides an ISO image centrally on the network in the form of a “virtual drive”.

  Remote Storage permits either the simultaneous connection of up to two “virtual” drives at the remote workstation or the provision of an ISO image via a Remote Storage server.

1.3 Communication interfaces of the iRMC S2/S3

The iRMC S2/S3 provides the following communication interfaces:

- **iRMC S2/S3 web interface (web interface)**

  The connection to the iRMC S2/S3 web server is established over a standard web browser (e.g. Microsoft Internet Explorer, Mozilla Firefox).

  Among other things, the web interface of the iRMC S2/S3 provides you with access to all system information and data from the sensors such as fan speeds, voltages, etc. You can also configure text-based console redirection and start graphical console redirection (Advanced Video Redirection, AVR). In addition, administrators can fully configure the iRMC S2/S3 over the web interface. Secure access to the iRMC S2/S3 web server can be provided with HTTPS/SSL.

  Operation of the iRMC S2/S3 over the web interface is described in chapter "iRMC S2/S3 web interface" on page 135.

- **Remote Manager: Text-based Telnet/SSH interface via LAN**

  You can call the Remote Manager

  – from the ServerView Remote Management Frontend,
  – directly from a Telnet/SSH client.

  The alphanumeric user interface of the Remote Manager provides you with access to system and sensor information, power management functions and the error event log. In addition, you can launch text console redirection or a SMASH CLP shell. If you call the Remote Manager over SSH (Secure Shell), the connection between the Remote Manager and the managed server is encrypted.

  Operation of the iRMC S2/S3 using the Remote Manager is described in chapter "iRMC S2/S3 via Telnet/SSH (Remote Manager)" on page 321.

- **Remote Manager (Serial): Text-based serial interface over Serial 1**

  The Remote Manager (serial) interface is identical to the Remote Manager interface.

1.4 Communication protocols used by the iRMC S2/S3

The communication protocols and ports used by the iRMC S2/S3 are shown in table 1.

Remote side of the connection	Communication direction	iRMC S2/S3 side of the connection (port number / protocol)
RMCP	→	623/UDP
	←	623/UDP
HTTP port	→	80/TCP
	←	80/TCP
HTTPs port	→	443/TCP
	←	443/TCP
Telnet	→	3172/TCP
	←	3172/TCP
SSH	→	22/TCP
	←	22/TCP
Trap	→	162/UDP
Email	→	25/TCP
	←	25/TCP
Remote Storage	→	5901/TCP
	←	5901/TCP
VNC ports		
Standard port	→	80/TCP
	←	80/TCP
Secure port	→	443/TCP
	←	443/TCP

Table 1: Communication protocols and ports used by the iRMC S2/S3

i As of iRMC S2/S3 firmware version 5.00, the Remote Storage port is used only for the Remote Storage server and client-internal communications. For integrated Remote Storage (via the Java applet), the http port is used.

1.5 IPMI - technical background

The iRMC S2/S3 makes the BMC functions available over the IPMI interface.

Intelligent Platform Management

The “Intelligent Platform Management” initiative is a response to the increasing complexity of modern server systems. A number of manufacturers have joined this initiative in order to come up with a new solution for monitoring these server systems.

The term “Intelligent Platform Management” expresses the core aspect of this approach to the solution: Functions for monitoring and recovery of systems are implemented directly in the hardware and firmware for platform management.

Objective

The objective was to define a standardized, abstract and message-based interface between the central system controller (Baseboard Management Controller - BMC) and intelligent platform management hardware.

The standardization committees combined the central characteristics of various platform management modules into standardized descriptions.

Definition

The IPMI specification defines:

> “IPMI is a hardware level interface specification that is ‘management software neutral’ providing monitoring and control functions that can be exposed through standard management software interfaces such as DMI, WMI, CIM, SNMP, etc. As a hardware level interface, it sits at the bottom of a typical management software stack” [see section "IPMI and other management standards" on page 22].

Advantage

The IPMI specifications ensure the independence of functions for inventory, logging, recovery and monitoring of a system by the system processor, BIOS or operating system.

This means that a system can still be involved in platform management when it is shut down and turned off.

IPMI and other management standards

IPMI is best used in conjunction with system management software running under the relevant operating system. Integration of the IPMI functionality into the management functionality offered by a management application and the operating system results in a powerful platform management environment.

An overview of the relationship between IPMI and the management software stack is shown by figure 2:

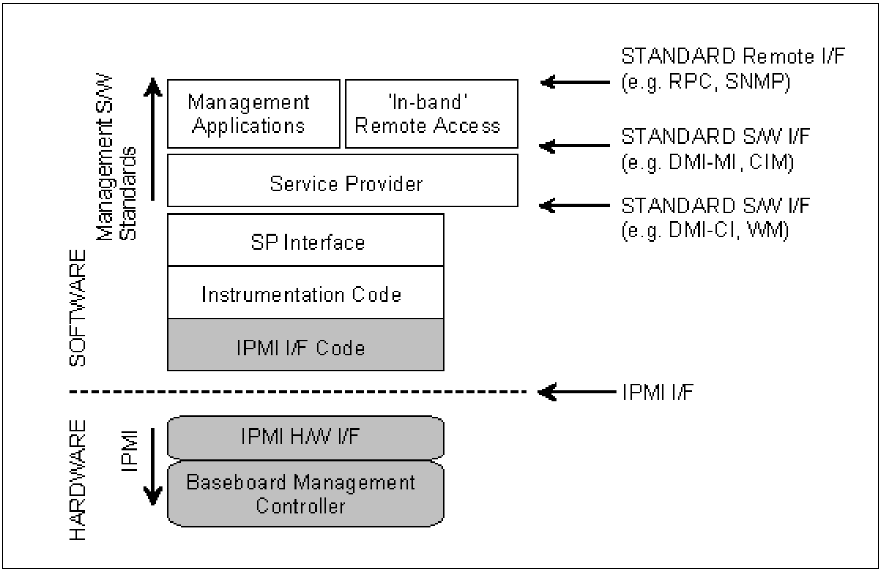


Figure 2: IPMI in the management software stack (source: IPMI specification, see section "References" on page 29)

IPMI, IPMB and ICMB

The IPMI initiative resulted in three central standards:

– *IPMI. Intelligent Platform Management Interface Specification*
  describes the higher-level architecture, the current commands, event formats, data packets and properties that are used in IPMI-based systems.

– *IPMB. Intelligent Platform Management Bus*
  is an I^{2}C based (write only) bus, which provides a standardized connection between various modules in a common housing.
  IPMB can also be used as a standardized interface for remote management modules.

– *ICMB. Intelligent Chassis Management Bus*
  (Not currently implemented in the ServerView remote management environment.)
  provides a standardized interface for exchange of platform management information and for control across systems. ICMB is designed in such a way that it can be implemented with a device that is connected to the IPMB.

IPMI implementation

The core element of an IPMI implementation is the Baseboard Management Controller (BMC).
The BMC performs the following tasks:

– The BMC organizes the interface between the system management software and the platform management hardware.

– It provides autonomous functions for monitoring, event logging and recovery control.

– The BMC acts as a gateway between the system management software and IPMB.

IPMI allows platform management to be extended: Additional management controllers can be connected via the IPMB. The IPMB is an I^{2}C based serial bus, which runs between the main modules of the system. It is used for communication with and between the management controllers.

With the support of multiple management controllers, IPMI provides a scalable architecture: A complex server system can use multiple controllers for monitoring different subsystems, e.g. power supplies, hot swap RAID drive modules etc.

In addition, IPMI provides ‘low level’ I^{2}C commands, which can be accessed via a management controller connected to the IPMB on 'unintelligent' I^{2}C modules that cannot process IPMI commands.

An overview of the fundamental elements of an IPMI implementation is available in figure 3 on page 25.

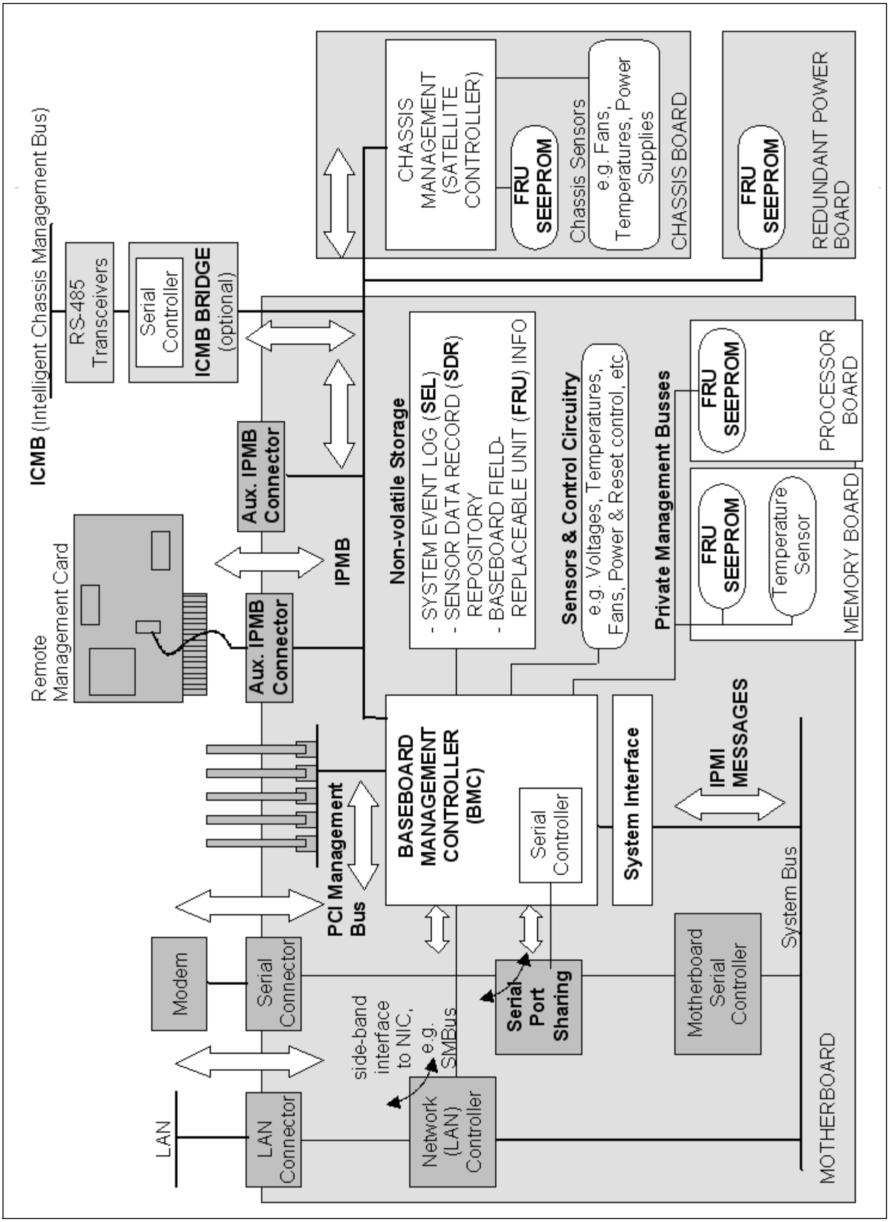


Figure 3: IPMI block diagram (source: IPMI specification, see section "References" on page 29)

IPMI and “in band” and “out of band” management

In the field of system management, a distinction is made between “in-band” and “out-of-band” management:

– The term “in-band” management is used when the operating system is running on the managed server.

– The term “out-of-band” management is used when the operating system is not running on the managed server, for instance if the hardware is faulty.

As different interfaces are available in an environment with IPMI compatible systems, you can manage IPMI compatible systems either “in band” or “out of band”.

IPMI-over-LAN

“IPMI-over-LAN” is the current name for the specification of the LAN interface in the IPMI standard. This specification stipulates how IPMI messages can be sent to or from the BMC of a managed system - encapsulated in RMCP (Remote Management Control Protocol) data packets. These RMCP data packets are transferred via an Ethernet LAN connection using the UDP (User Datagram Protocol) under IPv4 (Internet Protocol Version 4).

The RMCP protocol has been specified to support the management of system statuses in which the operating system is not running. The RMCP is a simple inquiry/response protocol.

The interface for such a connection is provided on an onboard LAN controller assigned to the BMC.

ℹ The interface can only be provided by an on-board LAN controller, not by an inserted LAN card.

Of the two ports that RCMP uses under UDP, the BMC communicates with the LAN controller via port 623 (primary RMCP Port).

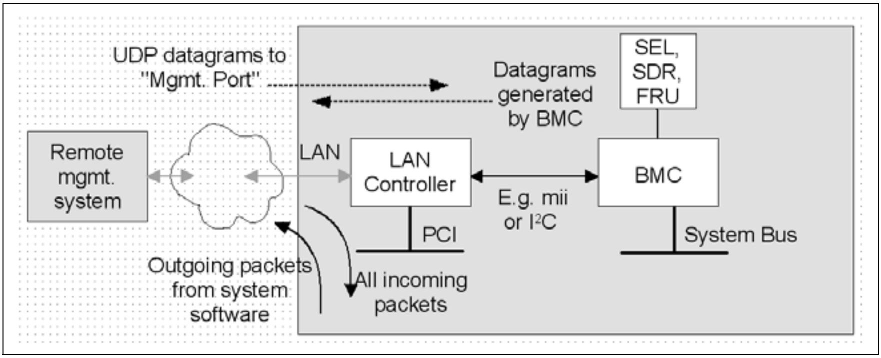


Figure 4: BMC and LAN controller

Serial Over LAN interface (SOL)

“Serial Over LAN” is an interface compliant with the IPMI V2.0 standard, which controls transfer of serial data over a LAN connection. In particular, SOL specifies the packet formats and protocols for transferring serial data streams over a LAN between the serial controller on the managed computer and a remote workstation. SOL is based on the IPMI-over-LAN specification.

In order to establish an SOL connection, a remote management application first initiates an IPMI-over-LAN session with the BMC. After this has been done, the SOL services can be activated from the remote workstation. The data traffic between the serial controller and the remote workstation is handled over the same IPMI session as the IPMI commands.

As soon as an SOL connection has been established, data transfer between the serial controller and the remote workstation is carried out as follows:

– Transfer from the serial controller to the remote workstation:
  The data stream issued by the serial controller is partitioned by the BMC, packaged and then sent to the remote workstation over the LAN.

– Transfer from the remote workstation to the serial controller:
  BMC unpacks the characters contained in the packages sent by the remote workstation and forwards them to the serial controller as a character stream.

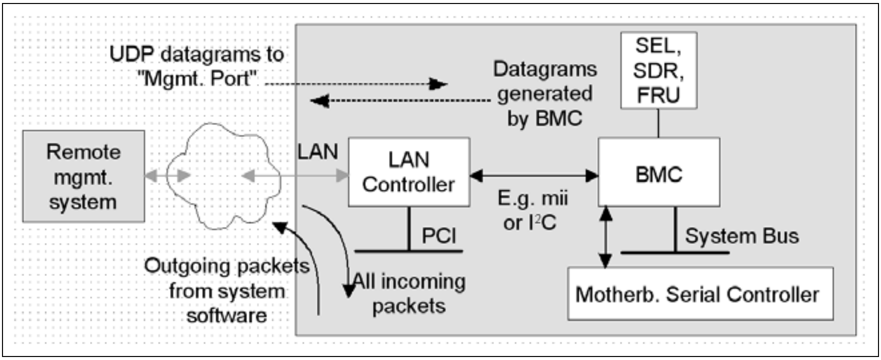

UDP datagrams to "Mgmt. Port"
Datagrams generated by BMC
SEL, SDR, FRU
Remote mgmt. system
LAN
LAN Controller
BMC
E.g. mii or I²C
PCI
System Bus
Outgoing packets from system software
All incoming packets
Motherb. Serial Controller

Figure 5: BMC and SOL

The SOL character data is then exchanged between the BMC of the managed system and the remote workstation as SOL messages. The SOL messages are encapsulated in RMCP+ data packets and transferred in UDP datagrams over an Ethernet LAN connection using IPv4 (Internet Protocol Version 4). The RMCP+ protocol is based on the RMCP protocol, but includes extensions for encryption, authentication, etc.

Serial over LAN permits “headless” management by console redirection by both the BIOS and the operating system of the managed server. High-cost concentrator solutions are not required.

Channel concept under IPMI

‘Channels’ provide the mechanisms with which IPMI messages are routed to the BMC via various connection carriers. Up to nine channels can be supported. The system interface and the primary IPMB are fixed. The other seven channels are available for the implementation.

Channels can be either ‘session based’ or ‘sessionless’. The ‘session’ concept has two meanings: It is either a concept for user authentication (see the section "User identifications" on page 29) or a concept for routing multiple IPMI message streams via a single channel.

Examples of ‘session based’ channels are LAN channels or serial / modem channels. Examples of ‘sessionless’ channels are the system interface and the IPMB.

User identifications

For ‘session based’ channels (see the section "Channel concept under IPMI" on page 28), a user login is necessary. By contrast, the ‘sessionless’ channels have no user authentication.

Under IPMI, the user configuration is channel specific. Thus, users can have different privileges depending on whether they are accessing the BMC via the LAN channel or the serial channel.

References

Information about the IPMI standards can be found on the Internet:

http://developer.intel.com/design/servers/ipmi/index.htm

1.6 DCMI (Data Center Management Interface)

The iRMC S2/S3 supports the DCMI (Data Center Management Interface) protocol, which is compliant with the IPMI V2.0 standard. DCMI has been designed to improve manageability and energy efficiency of server systems that are deployed in large data centers.

To meet the hardware management requirements of servers within data centers, DCMI supports, among others, the following key features:

- Inventory functions (server identification)
- Power Management and power monitoring
- Power consumption monitoring and control
- Event logging
- Temperature monitoring

Detailed information about DCMI can be found on the DCMI home page:

http://www.intel.com/technology/product/DCMI

1.7 Changes since the previous versions of the manual

iRMC S2/S3 - integrated Remote Management Controller (edition July 2012)

This manual refers to the iRMC S2/S3 **firmware version 6.5x** and replaces the following online manual: “iRMC S2/S3 - integrated Remote Management Controller”, May 2012 edition.

The manual includes the following updates:

- The "0 Watt Technology" feature is described in Chapter "7 iRMC S2/S3 web interface".
- The former chapter "12 IPMI OEM Commands" has been expanded and is now an Appendix ("12 Appendix") to the manual, containing the following sections:
  - "12.1 IPMI OEM Commands supported by the iRMC S2/S3" (former chapter "12 IPMI OEM Commands")
  - "12.2 Configuring the iRMC S2/S3 via SCCI and scripted configuration" (new section).

iRMC S2/S3 - integrated Remote Management Controller (edition May 2012)

This manual refers to the iRMC S2/S3 **firmware version 6.5x** and replaces the following online manual: “iRMC S2 - integrated Remote Management Controller”, November 2011 edition.

New iRMC S2/S3 features (described in Chapter "7 iRMC S2/S3 web interface"):

- Agentless HDD monitoring (iRMC S3 only)

  If the managed server supports the "agentless HDD monitoring" feature, the HDD<n> status of each individual HDD is directly read and reported to the iRMC S2/S3 via a dedicated lightpath status sensor and thus can be displayed even in the case no ServerView agents are running.

- Backing up/restoring BIOS settings, flashing BIOS

  If the BIOS of the managed server meets the corresponding feature requirements, the iRMC S2/S3 allows you to perform the following actions:

  - Backing up several BIOS parameters in ServerView® WinSCU XML format and restoring them in ServerView® WinSCU XML format from a file.
  - Updating BIOS via "upload from file" or via TFTP.

- For some server types, you can select the *Low Noise* mode under *Power Consumption Options* (iRMC S3 only).

iRMC S2/S3 - integrated Remote Management Controller (edition November 2011)

This manual refers to the iRMC S2/S3 **firmware version 5.5x** and replaces the following online manual: “iRMC S2 - integrated Remote Management Controller”, May 2011 edition.

The following topics are no longer part of this manual:

- Former section "4.4 Global user management for the iRMC S2/S3". As of SVOM V5.50, this section will be integrated in the "User Management in ServerView" manual.
- Description of the Server Configuration Manager dialog pages (former sections 9.2 and the following). Instead, the reader is advised to use the Online Help of the Server Configuration Manager.

iRMC S2/S3 - integrated Remote Management Controller (edition May 2011)

This manual refers to the iRMC S2/S3 **firmware version 5.5x** and replaces the following online manual: “iRMC S2 - integrated Remote Management Controller”, April 2011 edition.

The manual applies to both iRMC S2 and iRMC S3. Functional differences in between the iRMC S2 and the iRMC S3 are pointed out separately in the manual.

iRMC S2 - integrated Remote Management Controller (edition April 2011)

The April 2011 edition of the iRMC S2 manual refers to the iRMC S2 **firmware version 5.5x** and replaces the following online manual: “iRMC S2 - integrated Remote Management Controller”, July 2010 edition.

- New iRMC S2 features:

  - In addition to the system event log (IPMI SEL), the iRMC S2 now features an internal event log.
  - The iRMC S2 now supports both IPv4 and IPv6 addresses.
  - The iRMC S2 now supports the Open DS directory service.
  - iRMC S2 Configuration (iRMC S2 firmware settings) can be restored via the iRMC S2 web interface.
  - Email alerting is now also supported for global iRMCS2 user IDs.

- Chapter "5 Advanced Video Redirection (AVR)":

  In addition to some minor changes, the menu of the AVR window has been supplemented with the *Power Control* entry, allowing you now to power on / power down / reboot the server directly from the AVR window.

- Chapter "7 iRMC S2 web interface":

  - *Power Supply* page: The *Power Supply Redundancy Configuration* feature is available for some server types.
  - *System Event Log Content* page:

    GUI language "German":
    Event description and resolutions are described in German.

    GUI language "Japanese":
    Resolutions are described in Japanese.

  - The *DNS Configuration* page now additionally includes the functionality of the former *DHCP configuration* page, which is no longer available.
  - New / modified pages corresponding to the new iRMC S2 features mentioned above.

- Chapter "8 Remote Manager":

  New / modified menus corresponding to the new iRMC S2 features internal event log and IPv6 addressing.

- Chapter "9 Server Configuration Manager":

  New / modified menu pages corresponding to the new iRMC S2 features IPv6 addressing and Open DS support.

1.8 ServerView Suite link collection

Via the link collection, Fujitsu Technology Solutions provides you with numerous downloads and further information on the ServerView Suite and PRIMERGY servers.

For ServerView Suite, links are offered on the following topics:

- Forum
- Service Desk
- Manuals
- Product information
- Security information
- Software downloads
- Training

> The downloads include the following:
>
> – Current software versions for the ServerView Suite as well as additional Readme files.
>
> – Information files and update sets for system software components (BIOS, firmware, drivers, ServerView agents and ServerView update agents) for updating the PRIMERGY servers via ServerView Update Manager or for locally updating individual servers via ServerView Update Manager Express.
>
> – The current versions of all documentation on the ServerView Suite.
>
> You can retrieve the downloads free of charge from the Fujitsu Technology Solutions Web server.

For PRIMERGY servers, links are offered on the following topics:

- Service Desk
- Manuals
- Product information
- Spare parts catalogue

Access to the link collection

You can reach the link collection of the ServerView Suite in various ways:

1. Via ServerView Operations Manager.

   ► Select *Help – Links* on the start page or on the menu bar.

   This opens the start page of the ServerView link collection.

2. Via the ServerView Suite DVD 2 or via the start page of the online documentation for the ServerView Suite on the Fujitsu Technology Solutions manual server.

   i You access the start page of the online documentation via the following link:

   http://manuals.ts.fujitsu.com

   ► In the selection list on the left, select *Industry standard servers*.

   ► Click the menu item *PRIMERGY ServerView Links*.

   This opens the start page of the ServerView link collection.

3. Via the ServerView Suite DVD 1.

   ► In the start window of the ServerView Suite DVD 1, select the option *Select ServerView Software Products*.

   ► Click *Start*. This takes you to the page with the software products of the ServerView Suite.

   ► On the menu bar select *Links*.

   This opens the start page of the ServerView link collection.

1.9 Documentation for ServerView Suite

The documentation for the ServerView Suite can be found on the ServerView Suite DVD 2 supplied with each server system.

The documentation can also be downloaded free of charge from the Internet. You will find the online documentation at *http://manuals.ts.fujitsu.com* under the link *Industry standard servers*.

1.10 Notational conventions

The meanings of the symbols used in this manual are as follows:

⚠ **Warning**	This symbol is used to draw attention to risks which may represent a health hazard or which may lead to data loss or damage to the hardware.
ℹ	This symbol is used to highlight important information and tips.
▶	This symbol indicates an action which you must carry out.
Text in italics	In running text, commands, menu items, and the names of buttons, options, files and paths are shown in *italics*.
<text>	Indicates variables which must be replaced by current values.
`Monospaced font`	Output from the system is shown in `monospaced font`.

`Monospaced font`
`Bold monospaced font`
	Commands to be entered at the keyboard are shown in bold, monospaced font.

[square brackets]	Indicate optional entries.
{braces}	Indicate a list of alternatives separated by “|”.
[Keyboard] - [symbols]	Keys are shown as they appear on the keyboard. If uppercase characters are to be entered explicitly, this is indicated for instance by [SHIFT] - [A] for A. If two keys are to be pressed simultaneously, this is indicated by a hyphen between the two keyboard symbols.

Table 2: Notational conventions

If reference is made to passages elsewhere in this manual, the title of the chapter or section is named and the page number given refers to the start of the section.

2 Logging on to the iRMC S2/S3 for the first time

The factory default settings of the iRMC S2/S3 allow you to log in to the iRMC S2/S3 for the first time without the need for any configuration activities.

2.1 Requirements

On the remote workstation:

- Windows: Internet Explorer as of Version 7.x:
  Linux: Mozilla Firefox 3.x.
- For console redirection:
  Sun Java Virtual Machine Version 1.5.0_06 or higher.

In your network:

- You must have a DHCP server in your network.
- If you want to log in with a symbolic name rather than an IP address at the iRMC S2/S3 web interface, the DHCP server in your network must be configured for dynamic DNS.
- DNS must be configured. Otherwise you must ask for the IP address.

2.2 iRMC S2/S3 factory defaults

The firmware of the iRMC S2/S3 provides a default administrator ID and a default DHCP name for the iRMC S2/S3.

Default administrator ID:

Administrator ID:	admin
Password:	admin

Both the administrator ID and the password are case-sensitive.

For reasons of security, it is recommended that you create a new administrator account once you have logged in, and then delete the default administrator account or at least change the password for the account (see section "User Management" on page 263).

Default DHCP name of the iRMC S2/S3

The default DHCP name of the iRMC S2/S3 uses the following pattern:
IRMC<SerialNumber>

The serial number corresponds to the last 3 bytes of the MAC address of the iRMC S2/S3. You can take the MAC address of the iRMC S2/S3 from the label on your PRIMERGY server.

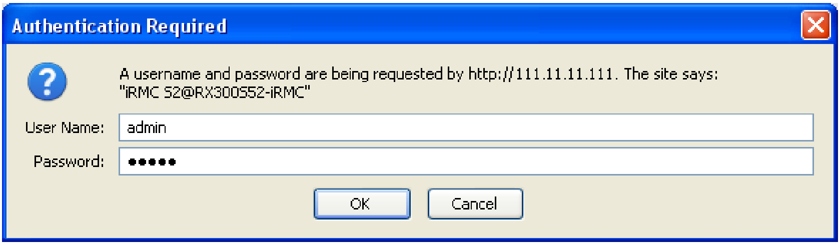
After you have logged in, the MAC address of the iRMC S2/S3 can be found as a read-only entry above the fields on the page *Network Interface* (see page 239).

2.3 Logging into the iRMC S2/S3 web interface

- ► Open a web browser on the remote workstation and enter the DNS name or IP address of the iRMC S2/S3.

  i You can take the DNS name of the iRMC S2/S3 from the label on your PRIMERGY server.

  The following login prompt appears:



Authentication Required

A username and password are being requested by http://111.11.11.111. The site says: "iRMC S2@RX300S52-iRMC"

User Name: admin

Password: •••••

Figure 6: Login prompt for the iRMC S2/S3 web interface

  i If the login prompt does not appear, check the LAN connection (see section "Testing the LAN interface" on page 47).

- ► Type in the data for the default administrator account.

  User name: admin

  Password: admin

- ► Click *OK* to confirm your entries.

The iRMC S2/S3 web interface opens showing the *System Information page* (see page 146).

3 Configuring the iRMC S2/S3

The following tools are available for configuring the iRMC S2/S3:

– BIOS / TrustedCore / UEFI setup utility (see page 44)

– iRMC S2/S3 web interface (see page 135)

– Server Configuration Manager (see page 347)

This chapter provides you with information about the following topics:

– Configuring the LAN interface of the iRMC S2/S3 using the BIOS / TrustedCore / UEFI setup utility (see page 44).

– Configuring text console redirection via LAN using the BIOS / TrustedCore / UEFI setup utility (see page 48).

– Configuring the serial interface of the iRMC S2/S3 using the BIOS / TrustedCore / UEFI setup utility (see page 57).

– Configuring the iRMC S2/S3 over the web interface (for an overview, see page 63).

3.1 Configuring the LAN interface of the iRMC S2/S3

This section describes:

– Requirements for configuring the LAN interface

– Configuring the LAN interface in the BIOS / TrustedCore® / UEFI setup utility

– Testing the LAN interface

"Spanning Tree" tree for the connection of the iRMC S2/S3 must be deactivated (e.g. Port Fast=enabled; Fast Forwarding=enabled).

3.1.1 Prerequisites

Note the following requirements with respect to configuring the IP address:

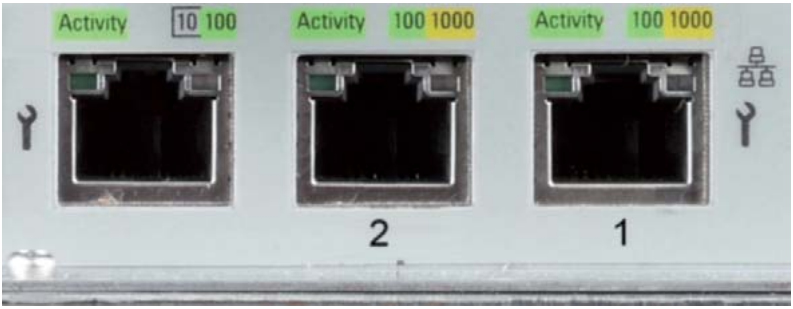
- The LAN cable must be connected to the correct port. (see section "Connected to the correct LAN port?" on page 42).
- Interaction between the IP addresses of the iRMC S2/S3 and the system (see the section "Interaction between the IP addresses of the iRMC S2/S3 and the system" on page 43).

3.1.1.1 Connected to the correct LAN port?

The interface for a LAN connection is provided on an onboard LAN controller assigned to the iRMC S2/S3 (see also figure 4 on page 27).

Depending on the server type, the system board of a PRIMERGY server provides two or three LAN interfaces. The ports marked with a wrench symbol are assigned to the iRMC S2/S3 (in figure 7, for example, these are port 1 and the top left-hand port).

> Check that the LAN cable is connected to the correct port.
>
> Depending on the type of PRIMERGY server, different ports may be marked with the wrench symbol.



Dedicated Service / Management LAN
(port exclusively for the iRMC S2/S3; with the iRMC S3 a LAN speed up to 1000 MBit/s is available, depending on the server hardware.)

(1) Shared LAN
(iRMC S2/S3 and system)

(2) LAN (port exclusively for the system)

Figure 7: Ports for the iRMC S2/S3 (indicated by wrench symbol)

3.1.1.2 Interaction between the IP addresses of the iRMC S2/S3 and the system

The LAN controller of the PRIMERGY server requires a separate IP address for the iRMC S2/S3 in order to ensure that data packets are reliably transferred to the iRMC S2/S3 (and not to the operating system).

The IP address of the iRMC S2/S3 must be different from that of the system (operating system).

3.1.1.3 Access from a different subnet

If the remote workstation accesses the iRMC S2/S3 of the managed server from a different subnet and DHCP is not used, you must configure the gateway.

3.1.2 Configuring the LAN interface: Configuration tools

You can configure the iRMC S2/S3's LAN interface in a number of ways:

Depending on the type of the PRIMERGY server

- using the BIOS / TrustedCore / UEFI setup utility (see page 44),
- iRMC S2/S3 web interface (see section "Network Settings - Configure the LAN parameters" on page 238),
- using the Server Configuration Manager (see chapter "Configuring iRMC S2/S3 using the Server Configuration Manager" on page 347).

3.1.3 Configuring the LAN interface using the BIOS / TrustedCore / UEFI setup utility

You can configure the iRMC S2/S3's LAN interface using the BIOS / TrustedCore / UEFI setup utility:

– Use the BIOS / TrustedCore setup utility to configure the LAN interface of the iRMC S2.

– Use the UEFI (**U**nified **E**xtensible **F**irmware **I**nterface) setup utility to configure the LAN interface of the iRMC S3.

3.1.3.1 Configuring the LAN interface of the iRMC S2 by using the BIOS / TrustedCore setup utility

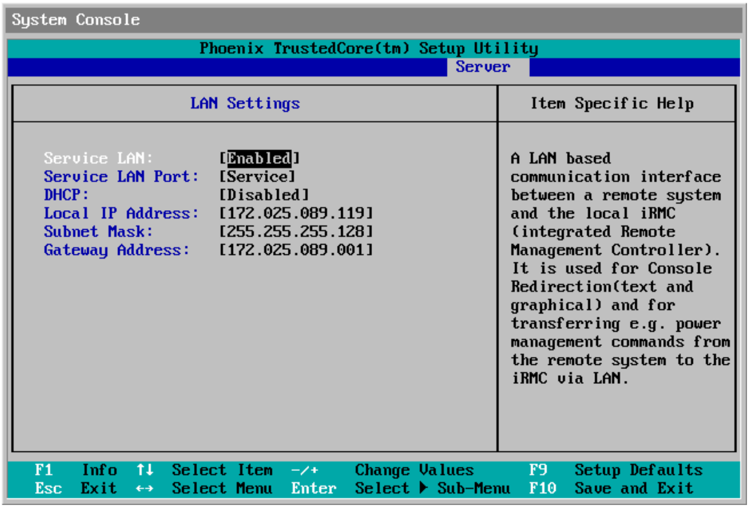
i IPv6 addresses are not supported in the BIOS / TrustedCore setup utility.

► Call the BIOS / TrustedCore setup utility of the managed server. Do this by pressing [F2] while the server is booting.

► Call the LAN parameter configuration menu:

  – BIOS: *Advanced – IPMI – LAN Settings*

  – TrustedCore: *Server – IPMI – LAN Settings*


System Console
Phoenix TrustedCore(tm) Setup Utility
Server
F1 Info ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▶ Sub-Menu F10 Save and Exit

```
LAN Settings                              Item Specific Help

Service LAN:         [Enabled]            A LAN based
Service LAN Port:    [Service]            communication interface
DHCP:                [Disabled]           between a remote system
Local IP Address:    [172.025.089.119]    and the local iRMC
Subnet Mask:         [255.255.255.128]    (integrated Remote
Gateway Address:     [172.025.089.001]    Management Controller).
                                          It is used for Console
                                          Redirection(text and
                                          graphical) and for
                                          transferring e.g. power
                                          management commands from
                                          the remote system to the
                                          iRMC via LAN.
```

Figure 8: LAN Settings menu (shown here for the TrustedCore setup utility)

► Configure the following settings:

Service LAN

Set the value to *Enabled*.

Service LAN Port

The *Service* setting is recommended.

ℹ The *Service* setting is mandatory for the Type TX150 S6 PRIMERGY server.

DHCP

If you enable DHCP, the iRMC S2 gets its LAN settings autonomously from a DHCP server on the network. In this case, the values for *Local IP Address*, *Subnet Mask*, etc. are set automatically.

ℹ Do not activate the DHCP option if no DHCP server is available. If you activate the DHCP option and there is no DHCP server available, the iRMC S2 goes into a search loop (i.e. it constantly searches for a DHCP server).You can specify that the DHCP and DNS services are to be used after initial installation, using the iRMC S2 web interface, for instance (see section "DNS Configuration - Configuring DNS for the iRMC S2/S3" on page 249).
By default, the following name is passed to the DHCP server on initial installation of the iRMC S3:

iRMC<last 3 bytes of the MAC address>.

Local IP Address

Enter the IP address you have determined for the iRMC S2 of the managed system.

Subnet Mask

Enter the subnet mask for the network. the iRMC S2 is connected to.

Gateway Address

Specify the IP address of the gateway of the network the iRMC S2 is connected to.

► Save the settings.

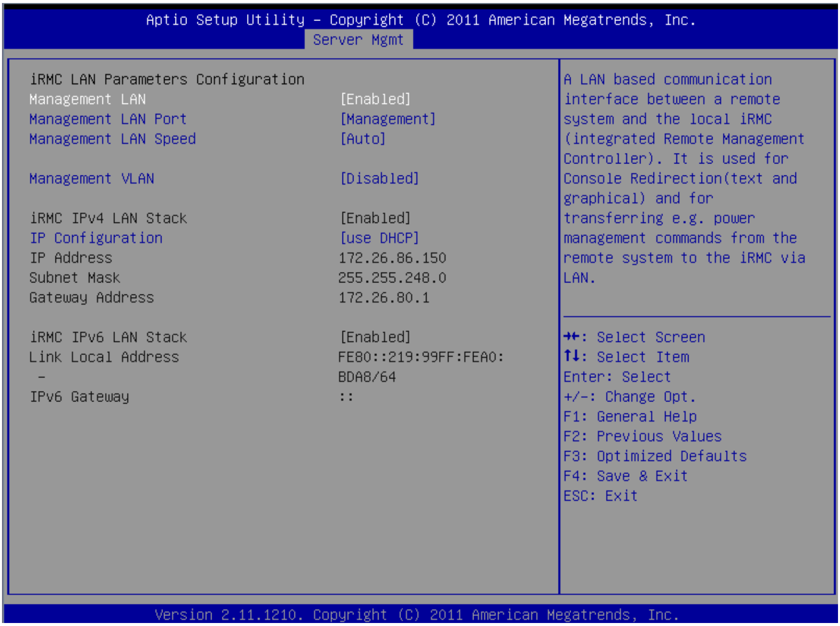
- ► If you want to use console redirection on the iRMC S2 continue with section "Configuring text console redirection for the iRMC S2" on page 49.

  If you do not want to use text console redirection on the iRMC S2, exit the BIOS/TrustedCore setup and continue with the next section "Testing the LAN interface".

3.1.3.2 Configuring the LAN interface of the iRMC S3 by using the UEFI setup Utility

- ► Call the UEFI setup utility of the managed server. Do this by pressing [F2] while the server is booting.
- ► Call the *iRMC LAN parameter configuration* menu:

  Server Mgmt – iRMC LAN Parameters Configuration



```
        Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
                                Server Mgmt

 iRMC LAN Parameters Configuration                     A LAN based communication
 Management LAN                  [Enabled]             interface between a remote
 Management LAN Port             [Management]          system and the local iRMC
 Management LAN Speed            [Auto]                (integrated Remote Management
                                                       Controller). It is used for
 Management VLAN                 [Disabled]            Console Redirection(text and
                                                       graphical) and for
 iRMC IPv4 LAN Stack             [Enabled]             transferring e.g. power
 IP Configuration                [use DHCP]            management commands from the
 IP Address                      172.26.86.150         remote system to the iRMC via
 Subnet Mask                     255.255.248.0         LAN.
 Gateway Address                 172.26.80.1

 iRMC IPv6 LAN Stack             [Enabled]             →←: Select Screen
 Link Local Address              FE80::219:99FF:FEA0:  ↑↓: Select Item
  -                              BDA8/64               Enter: Select
 IPv6 Gateway                    ::                    +/-: Change Opt.
                                                       F1: General Help
                                                       F2: Previous Values
                                                       F3: Optimized Defaults
                                                       F4: Save & Exit
                                                       ESC: Exit

        Version 2.11.1210. Copyright (C) 2011 American Megatrends, Inc.
```

Figure 9: iRMC LAN Parameters Configuration Menu

- Configure the following settings:

  Management LAN
  Set the value to *Enabled*.

  Management LAN Port
  The *Management* setting is recommended.

  ℹ For details on configuring the remaining settings see section "Network Settings - Configure the LAN parameters" on page 238 and/or refer to the manual "BIOS (Aptio) Setup Utility" manual corresponding to your server.

- Save the settings.

- If you want to use console redirection on the iRMC S3, continue with section "Configuring text console redirection for the iRMC S3" on page 53.

  If you do not want to use text console redirection on the iRMC S3, exit the UEFI setup and continue with the next section "Testing the LAN interface".

3.1.4 Testing the LAN interface

You can test the LAN interface as follows:

- Use a web browser to attempt to log into the iRMC S2/S3 web interface. If no login prompt appears, it is probable that the LAN interface is not working.

- Test the connection to the iRMC S2/S3 with a ping command.

3.2 Configuring text console redirection via LAN using the BIOS / TrustedCore / UEFI setup utility

Text console redirection will be available depending on the configuration of text console redirection and on the operating system of the server

– either for the duration of the BIOS POST phase only or

– beyond the BIOS POST phase while the operating system is running.

This section describes:

– Configuration of text console redirection via LAN using the BIOS / TrustedCore setup utility (for iRMC S2)

– Configuration of text console redirection via LAN using the UEFI setup utility (for iRMC S3)

– Special requirements of the operating system used that you need to take account of if you also want to use console redirection while the operating system is running.

ℹ You can also configure text console redirection via LAN using the iRMC S2/S3 web interface (see section "BIOS Text Console - Configure and start text console redirection" on page 292).

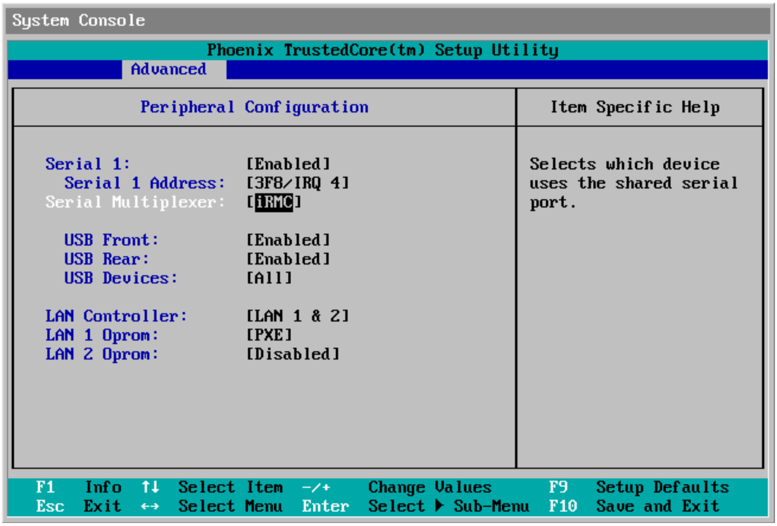
3.2.1 Configuring text console redirection for the iRMC S2

► Call the BIOS / TrustedCore setup utility of the managed server. Do this by pressing F2 while the server is booting.

Settings in the Peripheral Configuration menu

► Call the Peripheral Configuration menu:

Advanced – Peripheral Configuration



```
System Console
                 Phoenix TrustedCore(tm) Setup Utility
            Advanced
             Peripheral Configuration              Item Specific Help

   Serial 1:                [Enabled]             Selects which device
     Serial 1 Address:      [3F8/IRQ 4]           uses the shared serial
   Serial Multiplexer:      [iRMC]                port.

     USB Front:             [Enabled]
     USB Rear:              [Enabled]
     USB Devices:           [All]

   LAN Controller:          [LAN 1 & 2]
   LAN 1 Oprom:             [PXE]
   LAN 2 Oprom:             [Disabled]

  F1   Info  ↑↓  Select Item  -/+    Change Values       F9    Setup Defaults
  Esc  Exit  ↔   Select Menu  Enter  Select ▶ Sub-Menu   F10   Save and Exit
```

Figure 10: Peripheral Configuration menu (as it appears in the TrustedCore setup utility)

► Configure the following settings:

Serial 1

Set the value to *Enabled*.

Serial 1 Address

Accept the first value pair proposed.

Serial Multiplexer

Set the value to *iRMC*.

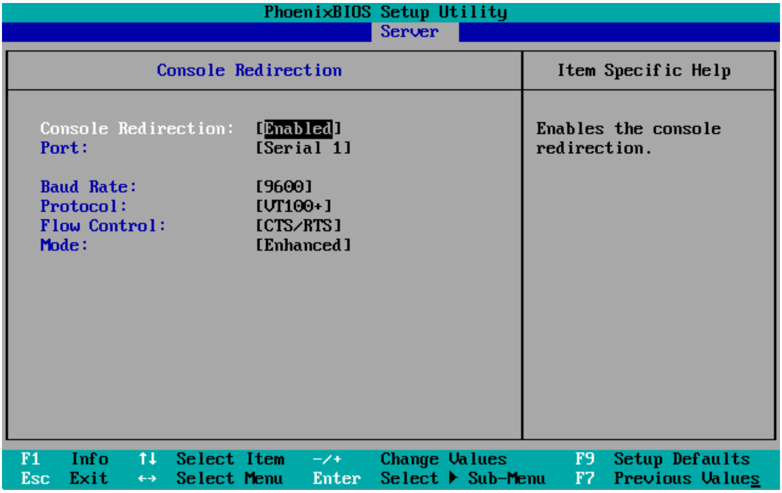
Settings in the Console Redirection menu

- ► Call the *Console Redirection* menu:

  Server – Console Redirection

  The appearance of the *Console Direction* menu varies depending on the setup utility (BIOS or TrustedCore) you are using.

- ► Make the following settings in the **BIOS setup utility**:



```
                         PhoenixBIOS Setup Utility
                                   Server
            Console Redirection                      Item Specific Help

    Console Redirection:    [Enabled]              Enables the console
    Port:                   [Serial 1]             redirection.

    Baud Rate:              [9600]
    Protocol:               [VT100+]
    Flow Control:           [CTS/RTS]
    Mode:                   [Enhanced]

 F1   Info   ↑↓  Select Item   -/+    Change Values         F9  Setup Defaults
 Esc  Exit   ↔   Select Menu   Enter  Select ▶ Sub-Menu     F7  Previous Values
```

Figure 11: Console Redirection menu (as it appears in the BIOS setup utility)

Console Redirection

Set the value to *Enabled*.

Port

Set the value to *Serial 1*.

Baud Rate

Specify the baud rate.

Protocol

Leave this setting unchanged. (The setting depends on the terminal type used.)

Flow Control

Leave this setting unchanged. (The setting depends on the terminal type used.)

Mode

This setting affects the behavior of console redirection while the operating system is running (after the POST phase has completed) - see section "Using console redirection while the operating system is running" on page 55:

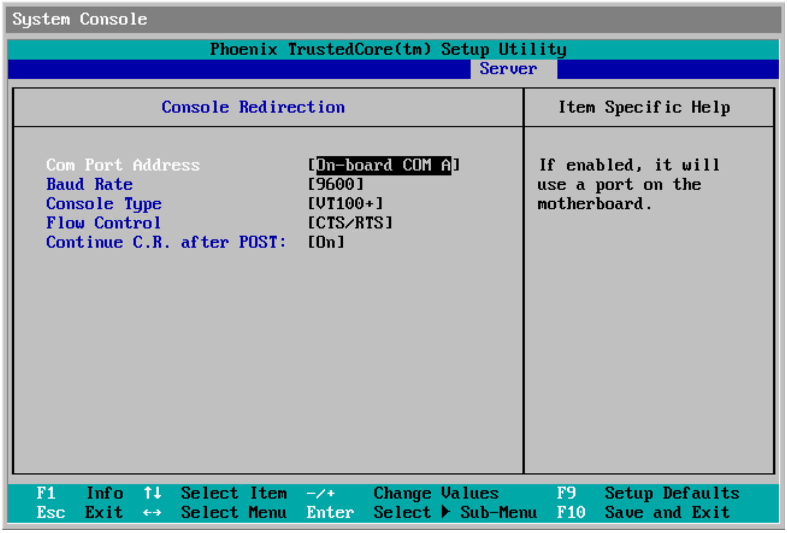
Standard

Console redirection is terminated after the BIOS POST phase.

Enhanced

Console redirection continues to be available after the BIOS POST phase.

► Make the following settings in the **TrustedCore setup utility**:



```
System Console
                 Phoenix TrustedCore(tm) Setup Utility
                                                  Server

              Console Redirection                    Item Specific Help

   Com Port Address              [On-board COM A]    If enabled, it will
   Baud Rate                     [9600]              use a port on the
   Console Type                  [VT100+]            motherboard.
   Flow Control                  [CTS/RTS]
   Continue C.R. after POST:     [On]

  F1   Info  ↑↓  Select Item  -/+    Change Values      F9   Setup Defaults
  Esc  Exit  ↔   Select Menu  Enter  Select ▶ Sub-Menu  F10  Save and Exit
```

Figure 12: Console Redirection menu (as it appears in the TrustedCore setup utility)

Com Port Address

Set the value to *On-board COM A*.

Baud Rate

Specify the baud rate.

Console Type

Leave this setting unchanged. (The setting depends on the terminal type used.)

Flow Control

The setting depends on the terminal type used. The settings must be the same on both terminal and managed server.

Continue C.R. after POST:

This setting affects the behavior of console redirection while the operating system is running (after the POST phase has completed) - see section "Using console redirection while the operating system is running" on page 55:

Off

Console redirection is terminated after the BIOS POST phase.

On

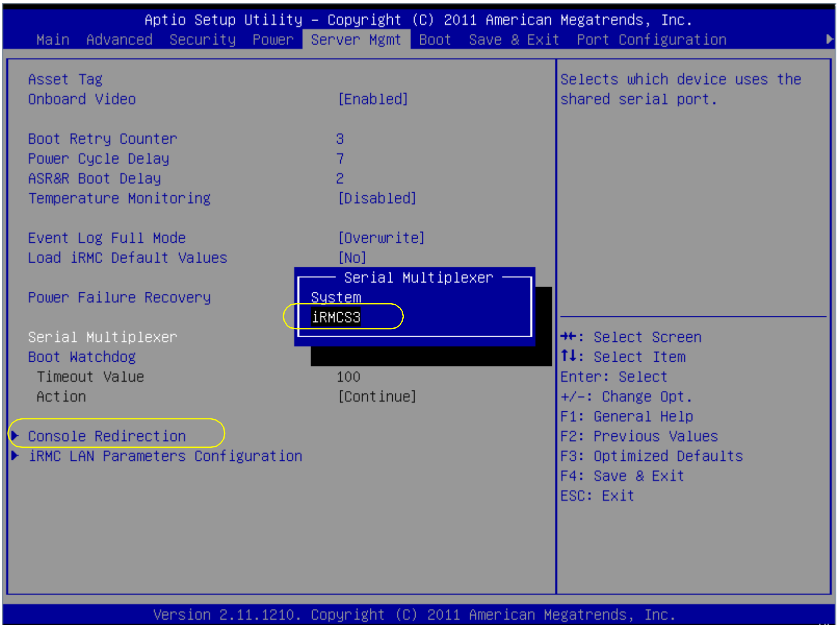
Console redirection continues to be available after the BIOS POST phase.

Exiting the BIOS / TrustedCore setup utility

- Save your settings and exit the BIOS/TrustedCore setup utility.
- Continue with section "Testing the LAN interface" on page 47.

3.2.2 Configuring text console redirection for the iRMC S3

- ► Call the UEFI setup utility of the managed server. Do this by pressing F2 while the server is booting.
- ► Call the *Server Mgmt* menu:



```
        Aptio Setup Utility – Copyright (C) 2011 American Megatrends, Inc.
  Main  Advanced  Security  Power  Server Mgmt  Boot  Save & Exit  Port Configuration  ►

  Asset Tag                                       Selects which device uses the
  Onboard Video                   [Enabled]       shared serial port.

  Boot Retry Counter              3
  Power Cycle Delay               7
  ASR&R Boot Delay                2
  Temperature Monitoring          [Disabled]

  Event Log Full Mode             [Overwrite]
  Load iRMC Default Values        [No]
                                  ── Serial Multiplexer ──
  Power Failure Recovery           System
                                   iRMCS3

  Serial Multiplexer                              →←: Select Screen
  Boot Watchdog                                   ↑↓: Select Item
   Timeout Value                  100             Enter: Select
   Action                         [Continue]      +/-: Change Opt.
                                                  F1: General Help
► Console Redirection                             F2: Previous Values
► iRMC LAN Parameters Configuration               F3: Optimized Defaults
                                                  F4: Save & Exit
                                                  ESC: Exit

        Version 2.11.1210. Copyright (C) 2011 American Megatrends, Inc.
```

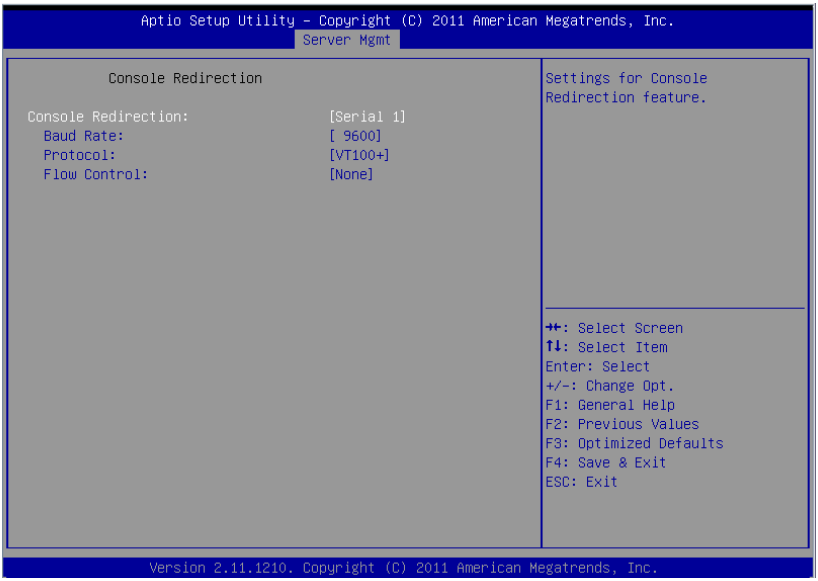
Figure 13: Server Mgmt Menu

- ► Make the following settings:

Serial Multiplexer

Set the value to *iRMCS3*.

- ► Call the *Console Redirection* menu:



```
Aptio Setup Utility – Copyright (C) 2011 American Megatrends, Inc.
                              Server Mgmt

          Console Redirection                       Settings for Console
                                                    Redirection feature.
 Console Redirection:                [Serial 1]
   Baud Rate:                        [ 9600]
   Protocol:                         [VT100+]
   Flow Control:                     [None]

                                                    →←: Select Screen
                                                    ↑↓: Select Item
                                                    Enter: Select
                                                    +/-: Change Opt.
                                                    F1: General Help
                                                    F2: Previous Values
                                                    F3: Optimized Defaults
                                                    F4: Save & Exit
                                                    ESC: Exit

     Version 2.11.1210. Copyright (C) 2011 American Megatrends, Inc.
```

Figure 14: Console Redirection menu

- ► Make the following settings in the *Console Redirection* menu:

Console Redirection

Set the value to *Serial 1*. In this case, the terminal uses the first serial interface.

Baud Rate

Specify the baud rate.

Protocol

Leave this setting unchanged. (The setting depends on the terminal type used.)

Flow Control

The setting depends on the terminal type used. The settings must be the same on both terminal and managed server.

Exiting the UEFI setup utility

- ► Save your settings and exit the UEFI setup utility.
- ► Continue with section "Testing the LAN interface" on page 47.

3.2.3 Using console redirection while the operating system is running

Depending on the operating system used on the managed server, you can continue to use console redirection after the BIOS POST phase.

DOS

The BIOS setting for console redirection mode must be set as follows (see section "Settings in the Console Redirection menu" on page 50):

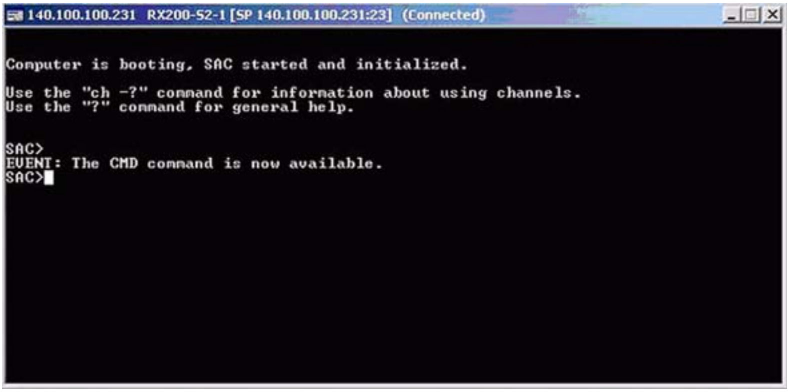
- BIOS setup utility: *Mode: Enhanced*
- TrustedCore setup utility: *Continue C.R. after POST: On*

Windows Server 2003 / 2008

If activated during Windows installation, console redirection is thereby automatically configured.

If console redirection is activated after Windows installation has completed, you must configure console redirection manually.

Windows Server 2003 / 2008 handles console redirection automatically after the POST phase. No further settings are necessary. While the operating system is booting, the Windows Server 2003 SAC console is transferred:



140.100.100.231 RX200-S2-1 [SP 140.100.100.231:23] (Connected)

```
Computer is booting, SAC started and initialized.

Use the "ch -?" command for information about using channels.
Use the "?" command for general help.


SAC>
EVENT: The CMD command is now available.
SAC>
```

Figure 15: Windows Server 2003 SAC console

Linux

You must configure a Linux operating system in such a way that it handles console redirection after the POST phase. Once it has been configured, you have unrestricted access from the remote workstation.

Settings required

The settings may differ between program versions.

SuSe and RedHat

Add the following line to the end of the file */etc/inittab*:

```
xx:12345:respawn:/sbin/agetty <baud-rate> ttyS0
```

RedHat

Insert the following kernel boot parameter in the file */etc/grub.conf*:

```
console=ttyS0,<baud-rate> console=tty0
```

SuSE

Insert the following kernel boot parameter in the file */boot/grub/menu.lst* :

```
console=ttyS0,<baud-rate> console=tty0
```

3.3 Configuring and using the serial interface of the iRMC S2/S3

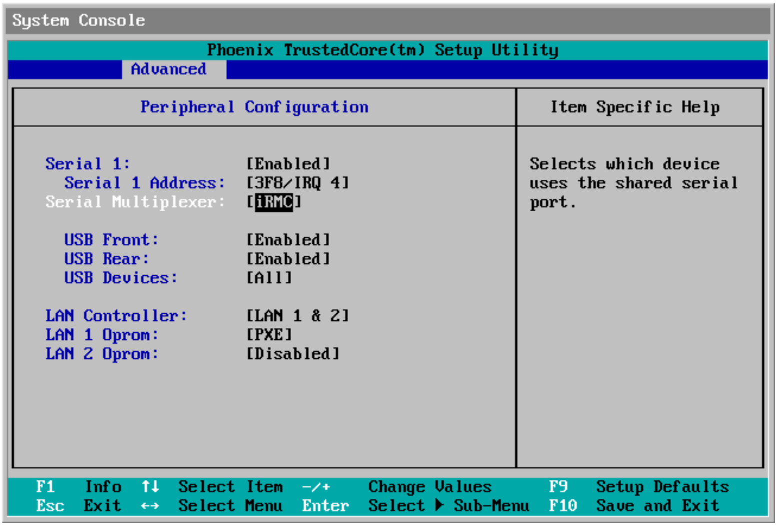
The serial interface of the iRMC S2/S3 offers you the following possibilities:

- You can use the terminal application Remote Manager (Serial) over a null modem cable (see section "Using the Remote Manager (Serial) interface" on page 62).
- In the case of an iRMC S2, you can forward alerts via modem. You can configure alerting via modem using the web interface of the iRMC S2 (see section "Serial / Modem Alerting - Configure alerting via modem" on page 255).

3.3.1 Configuring the serial interface of the iRMC S2

- Call the BIOS / TrustedCore setup utility of the managed server. Do this by pressing [F2] while the server is booting.
- Call the *Peripheral Configuration* menu to configure the serial port:

  Advanced – Peripheral Configuration



```
System Console
                    Phoenix TrustedCore(tm) Setup Utility
            Advanced
            Peripheral Configuration                    Item Specific Help

   Serial 1:                 [Enabled]            Selects which device
     Serial 1 Address:       [3F8/IRQ 4]          uses the shared serial
   Serial Multiplexer:       [iRMC]               port.

     USB Front:              [Enabled]
     USB Rear:               [Enabled]
     USB Devices:            [All]

   LAN Controller:           [LAN 1 & 2]
   LAN 1 Oprom:              [PXE]
   LAN 2 Oprom:              [Disabled]

   F1    Info  ↑↓  Select Item  -/+    Change Values        F9    Setup Defaults
   Esc   Exit  ↔   Select Menu  Enter  Select ▶ Sub-Menu    F10   Save and Exit
```

Figure 16: Peripheral Configuration menu (as it appears in the TrustedCore setup utility)

- Configure the following settings:

Serial 1

Set the value to *Enabled*.

Serial 1 Address

Accept the first value pair proposed.

Serial Multiplexer

Set the value to *iRMC*.

The following values are not shown in the menu and are preset (see page 62, “Terminal program (VT100+)”):

Bits per second
9600

Data bits
8

Parity
None.

Stop bits
1

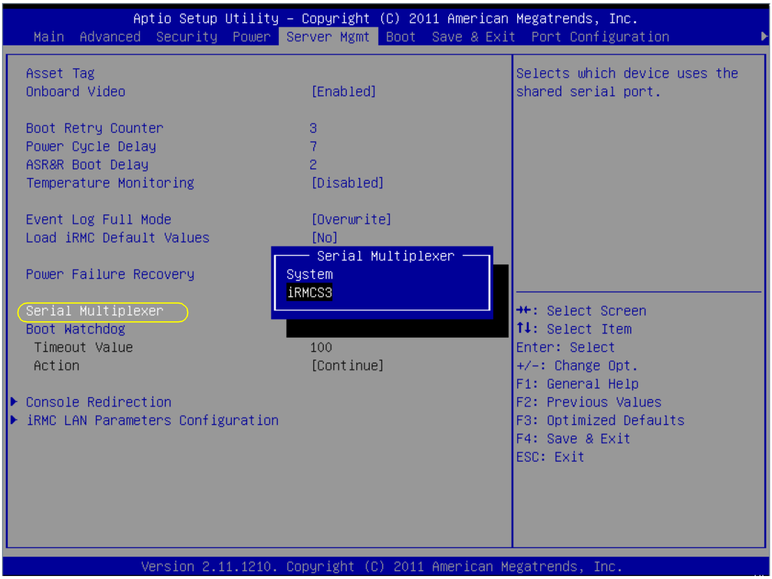
Flow Control
None

Exiting the BIOS / TrustedCore setup utility

- ► Save your settings and exit the BIOS/TrustedCore setup utility.
- ► Continue with section "Testing the LAN interface" on page 47.

3.3.2 Configuring the serial interface using of the iRMC S3

- ► Call the UEFI setup utility of the managed server. Do this by pressing [F2] while the server is booting.
- ► Call the *Server Mgmt* menu:



```
             Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
     Main  Advanced  Security  Power  Server Mgmt  Boot  Save & Exit  Port Configuration

  Asset Tag                                                 Selects which device uses the
  Onboard Video                      [Enabled]              shared serial port.

  Boot Retry Counter                 3
  Power Cycle Delay                  7
  ASR&R Boot Delay                   2
  Temperature Monitoring             [Disabled]

  Event Log Full Mode                [Overwrite]
  Load iRMC Default Values           [No]
                                  ─ Serial Multiplexer ─
  Power Failure Recovery           System
                                   iRMCS3
  Serial Multiplexer                                        →←: Select Screen
  Boot Watchdog                                             ↑↓: Select Item
   Timeout Value                     100                    Enter: Select
   Action                            [Continue]             +/-: Change Opt.
                                                            F1: General Help
► Console Redirection                                       F2: Previous Values
► iRMC LAN Parameters Configuration                         F3: Optimized Defaults
                                                            F4: Save & Exit
                                                            ESC: Exit

            Version 2.11.1210. Copyright (C) 2011 American Megatrends, Inc.
```

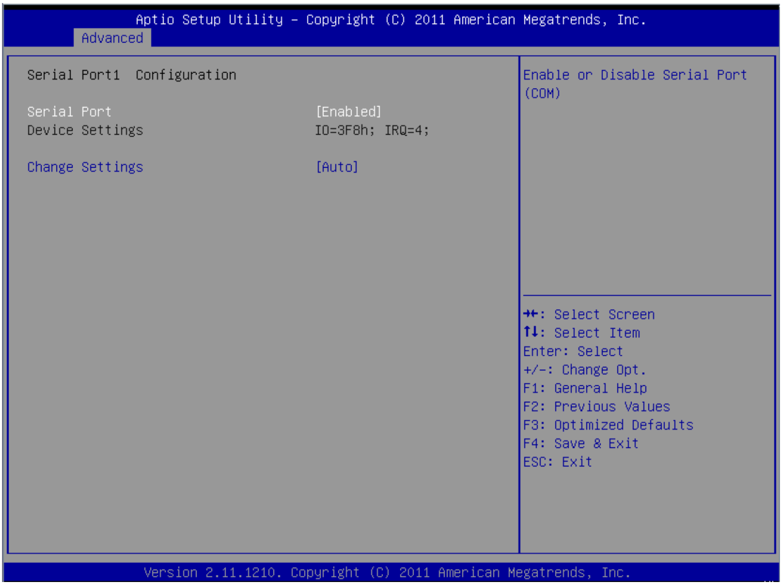
Figure 17: Server Mgmt menu

- ► Configure the following settings:

Serial Multiplexer
Set the value to *iRMCS3*.

- ► Call the *Serial Port 1 Configuration* menu to configure the serial port:

Advanced – Super IO Configuration – Serial Port 1 Configuration:



```
Aptio Setup Utility – Copyright (C) 2011 American Megatrends, Inc.
Advanced

Serial Port1  Configuration                        Enable or Disable Serial Port
                                                   (COM)
Serial Port                   [Enabled]
Device Settings               IO=3F8h; IRQ=4;

Change Settings               [Auto]

                                                   →←: Select Screen
                                                   ↑↓: Select Item
                                                   Enter: Select
                                                   +/-: Change Opt.
                                                   F1: General Help
                                                   F2: Previous Values
                                                   F3: Optimized Defaults
                                                   F4: Save & Exit
                                                   ESC: Exit

Version 2.11.1210. Copyright (C) 2011 American Megatrends, Inc.
```

Figure 18: Serial Port 1 Configuration menu

- ► Configure the following settings:

Serial Port

Set the value to *Enabled*.

Device Settings

Displays the base I/O address and the interrupt used to access the corresponding serial port, e.g. IO=3F8h; IRQ=4.

Accept the value pair proposed.

The following values are not shown in the menu and are preset (see page 62, “Terminal program (VT100+)”):

Bits per second

9600

Data bits

8

Parity

None.

Stop bits

1

Flow Control

None

Exiting the UEFI setup utility

- Save your settings and exit the UEFI setup utility.
- Continue with section "Testing the LAN interface" on page 47.

3.3.3 Using the Remote Manager (Serial) interface

If you connect a computer over a null modem cable and start a terminal program (VT100+) on this computer, you can access the Remote Manager (Serial) terminal program. The Remote Manager (Serial) interface is identical to the Remote Manager interface (see chapter "iRMC S2/S3 via Telnet/SSH (Remote Manager)" on page 321).

Prerequisites

On the managed server:

The *Serial Multiplexer* BIOS setting must be configured on the *iRMC* (see section "Configuring the serial interface of the iRMC S2" on page 58).

Terminal program (VT100+):

Configure the following port settings for the terminal program:

Bits per second

Set the value to *9600*.

Data bits

Set the value to *8*.

Parity

Set the value to *None*.

Stop bits

Set the value to *1*.

Flow Control

Set the value to *None*.

3.4 Configuring the iRMC S2/S3 over the iRMC S2/S3 web interface

- ► Start the iRMC S2/S3 web interface (see section "Logging into the iRMC S2/S3 web interface" on page 136).

3.4.1 Configuring the LAN parameters

- ► In the navigation area, click *Network Settings* (see section "Network Settings - Configure the LAN parameters" on page 238).

Configuring the LAN settings

- ► Configure the LAN settings on the *Network Interface* page. See the section "Network Interface Settings - Configure Ethernet settings on the iRMC S2/S3" on page 239 for the settings required.

Configuring ports and network services

- ► Configure the ports and network services on the *Ports and Network Services* page. See the section "Ports and Network Services - Configuring ports and network services" on page 245 for the settings required.

Configuring DHCP/DNS (Dynamic DNS)

- ► Configure the DHCP and DNS settings in the *DNS Configuration* page. See the section "DNS Configuration - Configuring DNS for the iRMC S2/S3" on page 249 for the settings required.

3.4.2 Configuring alerting

The pages for configuring alerting are grouped in the navigation area under *Alerting* (see section "Alerting - Configure alerting" on page 253).

Configuring alert forwarding over SNMP

- In the navigation area, click *SNMP Traps*. The *SNMP Traps* page appears.
- Configure SNMP trap forwarding. See the section "SNMP Trap Alerting - Configure SNMP trap alerting" on page 254 for the settings required.

Configuring alert forwarding to a mobile phone via modem (only with the iRMC S2)

- In the navigation area, click *Serial / Modem*. The *Serial / Modem Alerting* page appears.
- Configure alert forwarding via modem. See the section "Serial / Modem Alerting - Configure alerting via modem" on page 255 for the settings required.

Configuring email notification (email alerting)

- In the navigation area, click *Email*. The *Email Alerting* page appears.
- Configure email alerting. See the section "Email Alerting - Configure email alerting" on page 257 for the settings required.

3.4.3 Configuring text console redirection

- Configure text console redirection in the *BIOS Text Console* window. See the section "BIOS Text Console - Configure and start text console redirection" on page 292 for the settings required.

4 User management for the iRMC S2/S3

User management for the iRMC S2/S3 uses two different types of user identifications:

- **Local user identifications** are stored locally in the iRMC S2/S3's non-volatile storage and are managed via the iRMC S2/S3 user interfaces.
- **Global user identifications** are stored in the central data store of a directory service and are managed via this directory service's interfaces.

  The following directory services are currently supported for global iRMC S2/S3 user management:

  - Microsoft® Active Directory
  - Novell® eDirectory
  - OpenLDAP
  - OpenDS

This chapter provides information on the following topics:

- User management concept for the iRMC S2/S3
- User permissions
- Local user management on the iRMC S2/S3

i For detailed information on the global user management using the individual directory services, please refer to the "User Management in ServerView" manual.

4.1 User management concept for the iRMC S2/S3

User management for the iRMC S2/S3 permits the parallel administration of local and global user identifications.

When validating the authentication data (user name, password) which users enter when logging in to one of the iRMC S2/S3 interfaces, iRMC S2/S3 proceeds as follows (see also figure 19 on page 67):

1. The iRMC S2/S3 compares the user name and password with the locally stored user identifications:
   - If the user is authenticated successfully by iRMC S2/S3 (user name and password are valid) then the user can log in.
   - Otherwise, the iRMC S2/S3 continues the verification with step 2.
2. The iRMC S2/S3 authenticates itself at the directory service via LDAP with a user name and password, determines the user rights by means of an LDAP query and checks whether the user is authorized to work with these at the iRMC S2/S3.

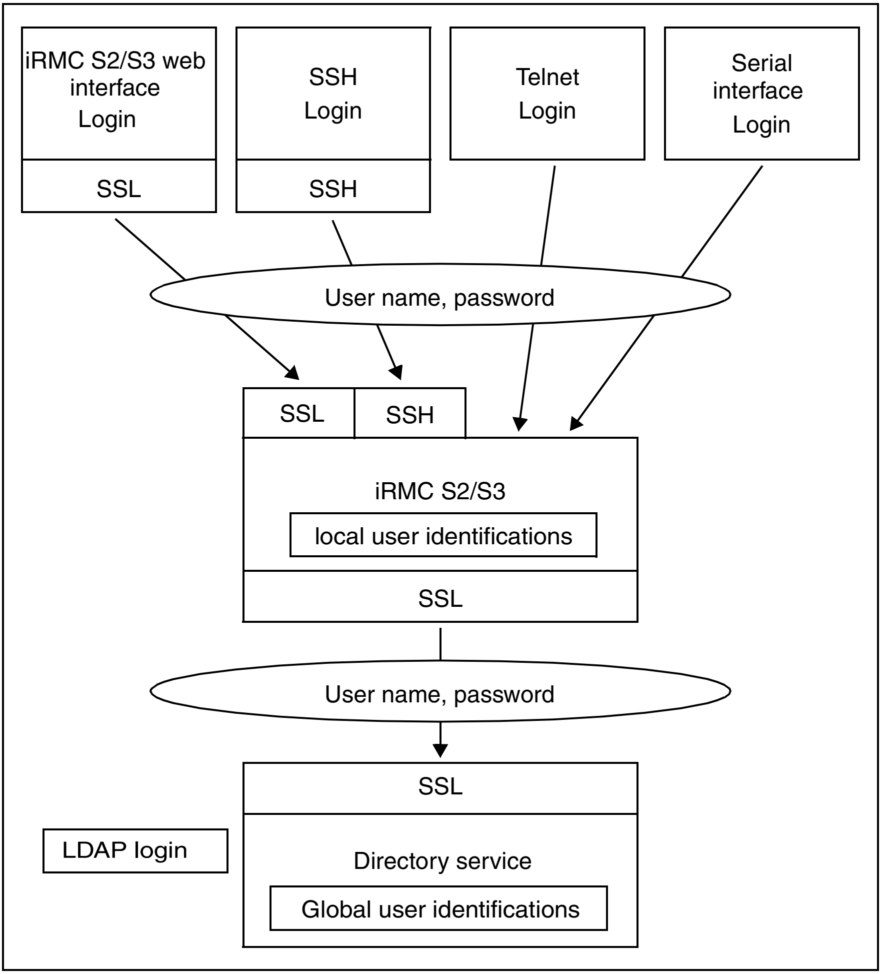


Bild 19: Login authentication via the iRMC S2/S3

i Although optional, the use of SSL for the LDAP connection between the iRMC S2/S3 and directory service is recommended. An SSL-secured LDAP connection between iRMC S2/S3 and the directory service guarantees secure data exchange, and in particular the secure transfer of the user name and password data.

SSL login via the iRMC S2/S3 web interface is only required if LDAP is active (*LDAP enable* option, see page 274).

4.2 User permissions

The iRMC S2/S3 distinguishes between two mutually complementary types of user permissions:

– Channel-specific privileges (via assignment to channel-specific permission groups)

– Permissions to use special iRMC S2/S3 functions

i The privileges and permissions required for the use of the individual iRMC S2/S3 functions are described

– for the iRMC S2/S3-web interface, on page 138,

– for the Remote Manager, on page 330.

Channel-specific privileges (channel-specific permission groups)

The iRMC S2/S3 assigns each user identification to one of the following four channel-specific permission groups:

– users
– Operator
– Administrator
– OEM

Since iRMC S2/S3 assigns these permissions on a channel-specific basis, users can have different permissions, depending on whether they access the iRMC S2/S3 over the LAN interface or the serial interface.

The scope of permissions granted increases from *User* (lowest permission level) through *Operator* and *Administrator* up to *OEM* (highest permission level).

i The permission groups correspond to the IPMI privilege level. Certain permissions (e.g. for Power Management) are associated with these groups or privilege levels.

Permissions to use special iRMC S2/S3 functions

In addition to the channel-specific permissions, you can also individually assign users the following permissions:

- **Configure User Accounts**
  Permission to configure local user identifications
- **Configure iRMC S2/S3 Settings**
  Permission to configure the iRMC S2/S3 settings.
- **Video Redirection Enabled**
  Permission to use Advanced Video Redirection (AVR) in “View Only” and “Full Control” mode
- **Remote Storage Enabled**
  Permission to use the Remote Storage functionality

Preconfigured user ID

The firmware of the iRMC S2/S3 provides a default administrator ID for the iRMC S2/S3 which possesses all permissions:

Administrator ID:	admin
Password:	admin

Both the administrator ID and the password are case-sensitive in the case of local users.

It is urgently recommended that you create a new administrator account as soon as possible once you have logged in, and then delete the default administrator account or at least change the password for the account (see section "User Management" on page 263).

4.3 Local user management for the iRMC S2/S3

The iRMC S2/S3 possesses its own local user management. Up to 16 users to be configured with passwords and be assigned various rights depending on the user groups they belong to. The user identifications are stored in the iRMC S2/S3’s local, non-volatile storage.

The following options are available for user management on the iRMC S2/S3:

- User management via the web interface
- User management via the Server Configuration Manager

4.3.1 Local user management using the iRMC S2/S3 web interface

i User management on the iRMC S2/S3 requires *Configure User Accounts* permission.

You can view a list of configured users under the web interface. You can also configure new users, change the configuration of existing users and remove users from the list.

► Start the iRMC S2/S3 web interface (see section "Logging into the iRMC S2/S3 web interface" on page 136).

Showing the list of configured users

► In the navigation area, click the *User Management - iRMC S2/S3 User* function.

The *User Management* page opens containing a list of configured users (see page 264). Here, you can delete users and call the page for configuring new users.
This page is described in section "User Management" on page 263.

Configuring new users

- ► On the *User Management* page, click the *New User* button.

  The *New User Configuration* page opens. This page allows you to configure the basic settings for the new user. This page is described in section "New User Configuration - Configuring a new user" on page 265.

Modifying the configuration of a user

- ► On the *User Management* page, click the name of the user whose configuration parameters you want to change.

  The *User "<name>" Configuration* page opens showing the settings for the selected user. Here, you can change the configuration parameters for the new user. This page is described in section "User "<name>" Configuration - User configuration (details)" on page 266.

Deleting users

- ► On the *User Management* page, click on the *Delete* button in the same line as the user to be deleted.

4.3.2 Local user management via the Server Configuration Manager

i **Prerequisite:**

The current ServerView agents must be installed on the managed server.

i User management on the iRMC S2/S3 requires *Configure User Accounts* permission.

User management via the Server Configuration Manager largely conforms to user management using the iRMC S2/S3 web interface.

In chapter "Configuring iRMC S2/S3 using the Server Configuration Manager" on page 347 is described how to start the Server Configuration Manager.

For details on the individual Configuration Manager dialogs, please refer to the online help of the Server Configuration Manager.

4.3.3 SSHv2 public key authentication for iRMC S2/S3 users

In addition to authentication by means of a user name and password, the iRMC S2/S3 also supports SSHv2-based public key authentication using pairs of public and private keys for local users. To implement SSHv2 public key authentication, the SSHv2 key of an iRMC S2/S3 user is uploaded to the iRMC S2/S3 and the iRMC S2/S3 user uses their private key with the program *PuTTY* or the OpenSSH client program *ssh*, for example.

The iRMC S2/S3 supports the following types of public keys:

- SSH DSS (minimum requirement)
- SSH RSA (recommended)

The public SSHv2 keys that you upload to the iRMC S2/S3 can be available either in RFC4716 format or in OpenSSH format (see page 84).

Public key authentication

In outline, public key authentication of a user on the iRMC S2/S3 happens as follows:

The user who wishes to log into the iRMC S2/S3 creates the key pair:

- The private key is read-protected and remains on the user's computer.
- The user (or administrator) uploads the public key to the iRMC S2/S3.

If the configuration allows this, the user can now log into the iRMC S2/S3 extremely securely and without the need to enter a password. The user is only responsible for keeping their private key secret.

The following steps are necessary to set up private key authentication. They are described in the subsequent sections:

1. Creating the public and private SSHv2 keys with the program *PuTTYgen* or *ssh-keygen* and saving them in separate files (see page 73).
2. Loading the public SSHv2 key onto the iRMC S2/S3 from a file (see page 77).
3. Configuring the program *PuTTY* or *ssh* for SSHv2 access to the iRMC S2/S3 (see page 79).

4.3.3.1 reating public and private SSHv2 keys

You can create public and private SSHv2 keys

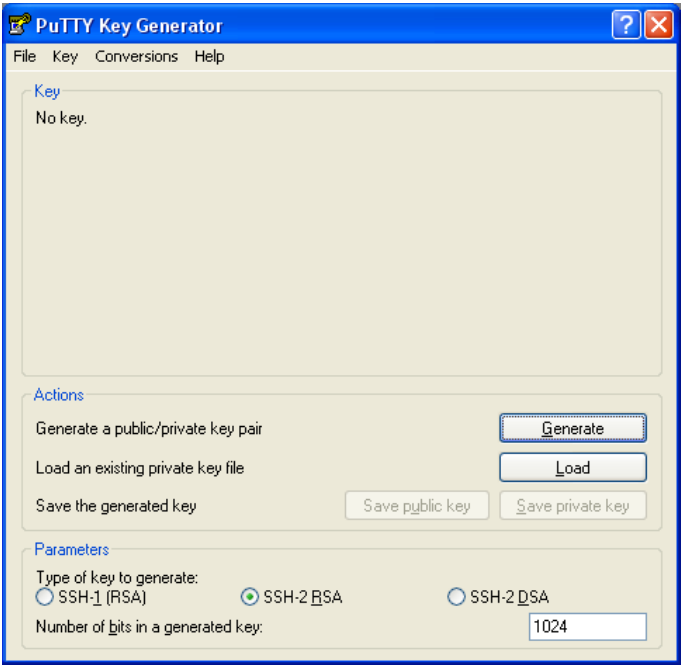
- with the program *PuTTYgen* or
- with the OpenSSH client program *ssh-keygen*.

Creating the public and private SSHv2 keys with PuTTYgen

Proceed as follows:

► Start *PuTTYgen* on your Windows computer.

The following window appears when *PuTTYgen* is started:



No key.

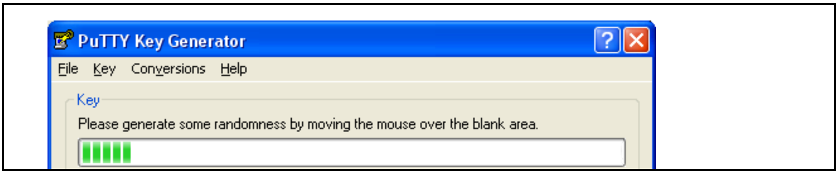
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

Bild 20: PuTTYgen: Creating new private and public SSHv2 keys

► Under *Parameters*, select the key type *SSH-2RSA* and click *Generate* to start generation of the keys.

The progress of the generation operation is then displayed under *Key* (see figure 21 on page 74).

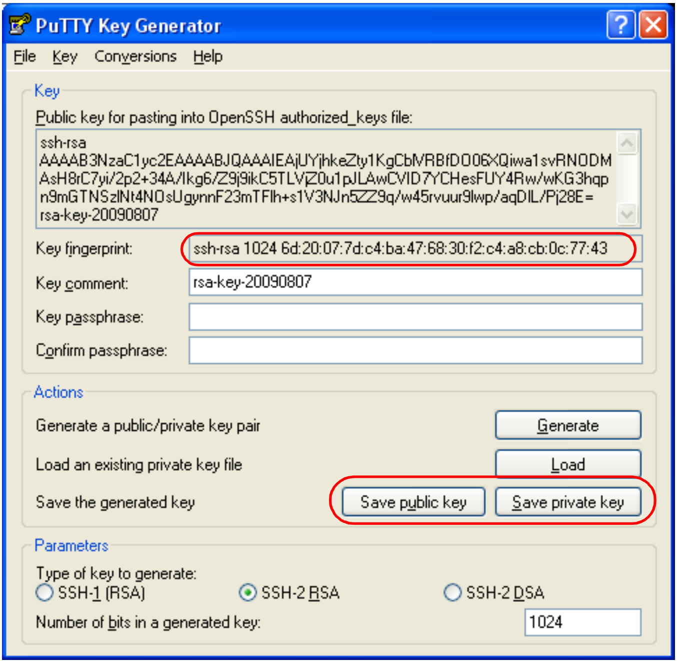


Please generate some randomness by moving the mouse over the blank area.

Bild 21: PuTTYgen: Creating a new key pair (progress bar).

- ► Move the mouse pointer over the blank area of the progress display to increase the randomness of the generated keys.

  When the keys have been generated, *PuTTYgen* displays the key and the fingerprint of the public SSHv2 key:



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEAjUYjhkeZty1KgCbMRBfDO06XQiwa1svRNODM
AsH8rC7yi/2p2+34A/Ikg6/Z9j9ikC5TLVjZ0u1pJLAwCVID7YCHesFUY4Rw/wKG3hqp
n9mGTNSzlNt4NOsUgynnF23mTFlh+s1V3NJn5ZZ9q/w45rvuur9lwp/aqDIL/Pj28E=
rsa-key-20090807
```

Key fingerprint: ssh-rsa 1024 6d:20:07:7d:c4:ba:47:68:30:f2:c4:a8:cb:0c:77:43

Key comment: rsa-key-20090807

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

Bild 22: PuTTYgen: Creating a new private SSHv2 key (progress bar).

- ► Click *Save public key* to save the public SSHv2 key to a file. You can upload the public key to the iRMC S2/S3 from this file (see page 77).
- ► Click *Save private key* to save the private SSHv2 key to a file for use with *PuTTY* (see page 79).

Creating the public and private SSHv2 keys with ssh-keygen

> i If it is not already pre-installed in the Linux distribution you are using, you can obtain OpenSSH from *http://www.openssh.org*.
>
> You will find a detailed description of the operands in the OpenSSH OpenSSH manual pages under *http://www.openssh.org/manual.html*

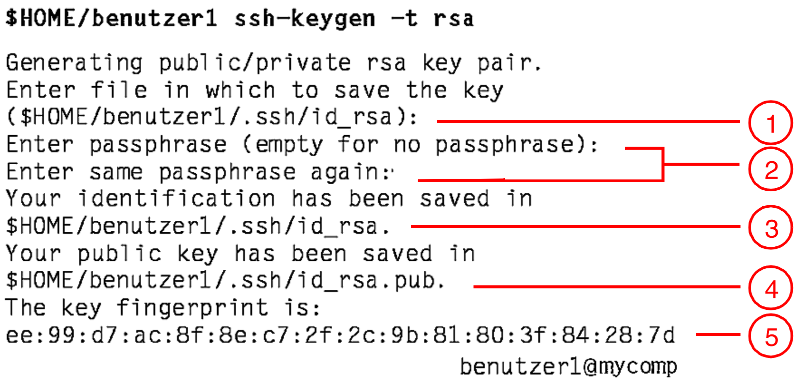
Proceed as follows:

► Call *ssh-keygen* to generate an RSA key pair:

```
ssh-keygen -t rsa
```

ssh-keygen logs the progress of the key generation operation. *ssh-keygen* queries the user for the file name under which the private key is to be stored and for the passphrase for the private key. *ssh-keygen* stores the resulting private and public SSHv2 keys in separate files and displays the fingerprint of the public key.

Example: Generating an RSA key pair with ssh -keygen



```
$HOME/benutzer1 ssh-keygen -t rsa

Generating public/private rsa key pair.
Enter file in which to save the key
($HOME/benutzer1/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
$HOME/benutzer1/.ssh/id_rsa.
Your public key has been saved in
$HOME/benutzer1/.ssh/id_rsa.pub.
The key fingerprint is:
ee:99:d7:ac:8f:8e:c7:2f:2c:9b:81:80:3f:84:28:7d
                                benutzer1@mycomp
```

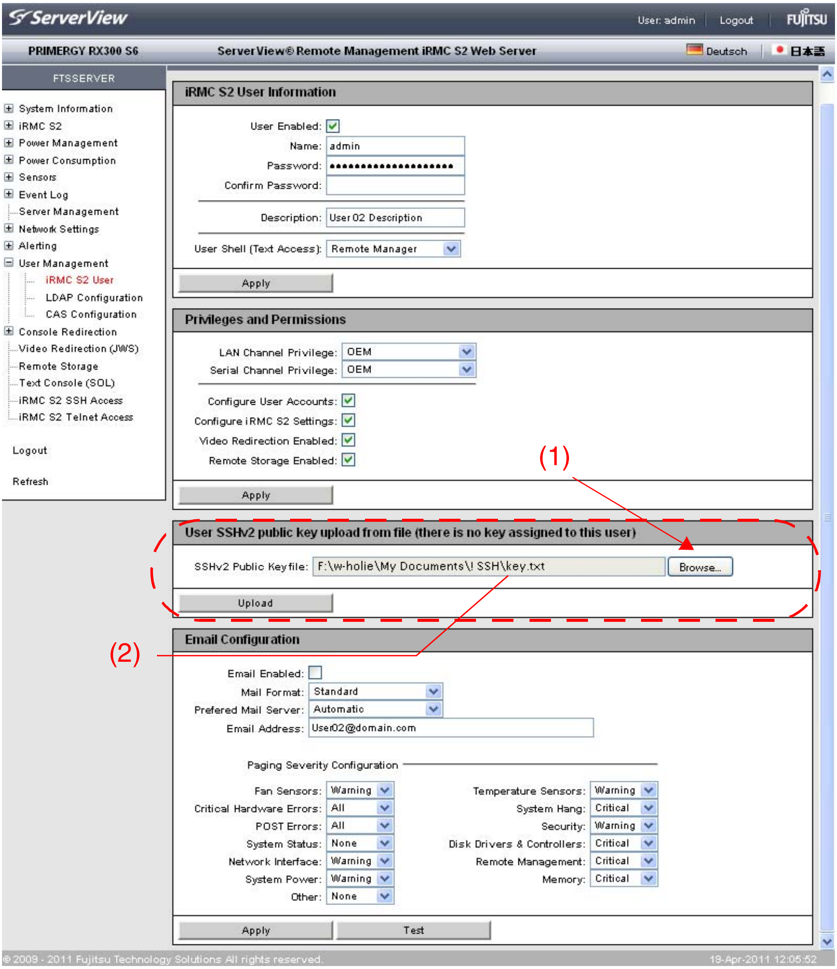
Explanation:

1. *ssh-keygen* requests the file name under which the SSHv2 key is to be saved. If you press Enter to confirm without entering a file name, *ssh-keygen* uses the default file name *id_rsa*.
2. *ssh-keygen* requests you to enter a passphrase (and to confirm it) that is used to encrypt the private key. If you press Enter to confirm without entering a passphrase, *ssh-keygen* does not use a passphrase.
3. *ssh-keygen* informs the user that the newly generated private SSHv2 key has been saved in the file */.ssh/id_rsa*.
4. *ssh-keygen* informs the user that the newly generated public SSHv2 key has been saved in the file */.ssh/id_rsa.pub*.
5. *ssh-keygen* displays the fingerprint of the public SSHv2 key and the local login to which the public key belongs.

4.3.3.2 Loading the public SSHv2 key onto the iRMC S2/S3 from a file

Proceed as follows:

- ► Under the iRMC S2/S3 web interface, open the detailed view for the required browser (in this case *user3*) *iRMC S2/S3 User Management* page:



iRMC S2 User Information

User Enabled: ☑
Name: admin
Password: ••••••••••••••••••••
Confirm Password:
Description: User 02 Description
User Shell (Text Access): Remote Manager

Privileges and Permissions

LAN Channel Privilege: OEM
Serial Channel Privilege: OEM
Configure User Accounts: ☑
Configure iRMC S2 Settings: ☑
Video Redirection Enabled: ☑
Remote Storage Enabled: ☑

User SSHv2 public key upload from file (there is no key assigned to this user)

SSHv2 Public Key file: F:\w-holie\My Documents\! SSH\key.txt

Email Configuration

Email Enabled: □
Mail Format: Standard
Prefered Mail Server: Automatic
Email Address: User02@domain.com

Paging Severity Configuration

Fan Sensors: Warning
Critical Hardware Errors: All
POST Errors: All
System Status: None
Network Interface: Warning
System Power: Warning
Other: None
Temperature Sensors: Warning
System Hang: Critical
Security: Warning
Disk Drivers & Controllers: Critical
Remote Management: Critical
Memory: Critical

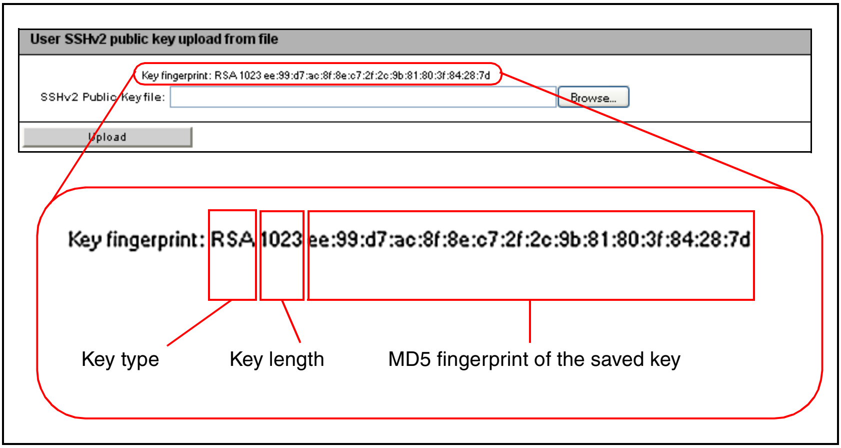
© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.   19-Apr-2011 12:05:52

Bild 23: iRMC S2/S3 web interface: Loading the public SSHv2 key onto the iRMC S2/S3

- ► Click *Browse* in the group *User SSHv2 public key upload from file* (1) and navigate to the file containing the required public key (2).

► Click *Upload* to load the public key onto the iRMC S2/S3.

After the key has been successfully uploaded, the iRMC S2/S3 displays the key fingerprint in the group *User SSHv2 public key upload from file*:



User SSHv2 public key upload from file

Key fingerprint: RSA 1023 ee:99:d7:ac:8f:8e:c7:2f:2c:9b:81:80:3f:84:28:7d

SSHv2 Public Key file:

Bild 24: Display of the key fingerprint

For reasons of security, make sure that the fingerprint shown here matches that shown in *PuTTYgen* (see figure 22 on page 74) under *Key fingerprint*.

4.3.3.3 Configuring PuTTY and the OpenSSH client for using the public SSHv2 key

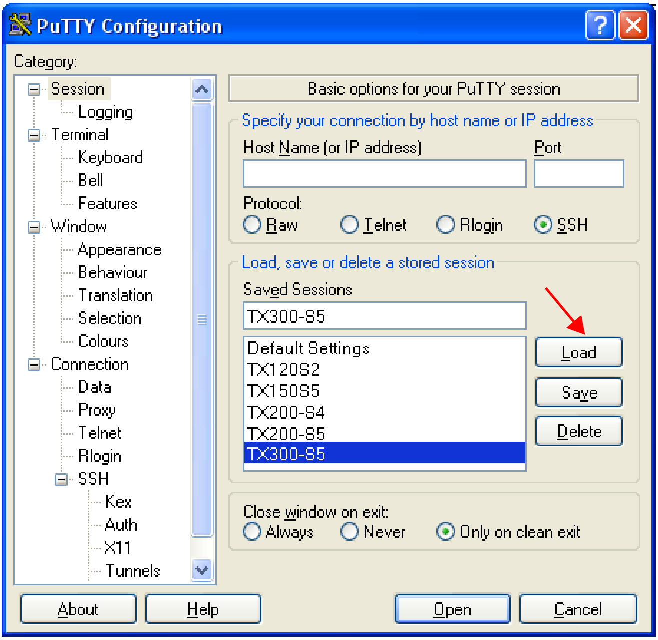
Configuring PuTTY for using the public SSHv2 key

The *PuTTY* program allows you to set up a public-key-authenticated connection to the iRMC S2/S3 and log in either under your user name or using the auto-login mechanism. *PuTTY* handles the authentication protocol automatically on the basis of the public/private SSHv2 key pair previously generated.

Proceed as follows:

- ► Start *PuTTY* on your Windows computer.

  The following window appears when *PuTTY* is started:



Host Name (or IP address):

Port:

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Saved Sessions: TX300-S5

Default Settings
TX120S2
TX150S5
TX200-S4
TX200-S5
TX300-S5

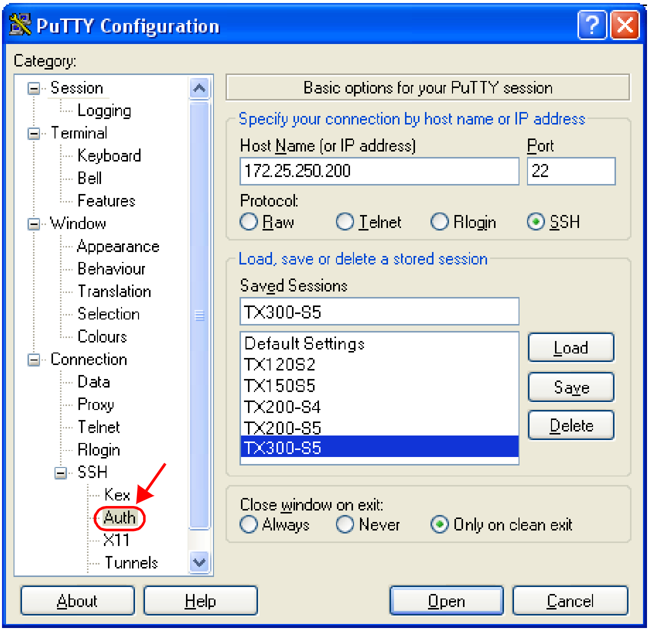
Close window on exit: ○ Always ○ Never ● Only on clean exit

Bild 25: PuTTY: Selecting and loading an SSH session

- ► Select a saved SSH session or create a new SSH session for the iRMC S2/S3 for which you want to use the SSHv2 key.

- ► Click *Load* to load the selected SSH session.

This opens the following window:



Host Name (or IP address): 172.25.250.200

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Saved Sessions: TX300-S5

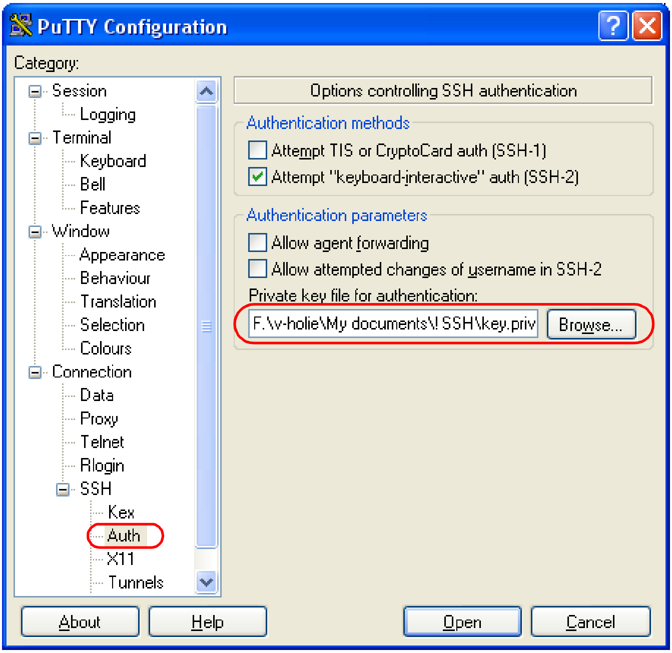
Default Settings
TX120S2
TX150S5
TX200-S4
TX200-S5
TX300-S5

Close window on exit: ○ Always ○ Never ● Only on clean exit

Bild 26: PuTTY: Loading an SSH session

- ► Choose *SSH - Auth* to configure the SSH authentication options.

This opens the following window (see figure 27 on page 81).



Options controlling SSH authentication

Authentication methods

☐ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding

☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

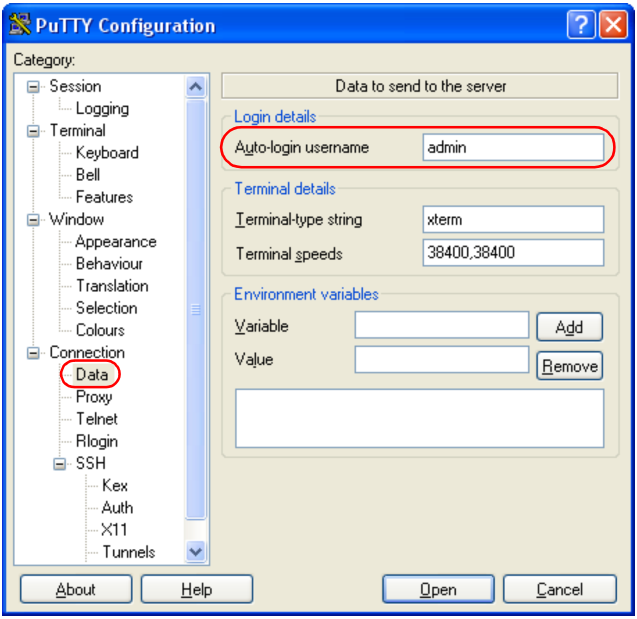
F:\v-holie\My documents\! SSH\key.priv

Bild 27: Configuring the SSH authentication options

► Select the file containing the private key that you want to use with the iRMC S2/S3.

i **Please note:**
At this point, you require the private key (see page 74) and **not** the public key that you loaded onto the iRMC S2/S3.

Under *Connection - Data*, you can additionally specify a user name for automatic login onto the iRMC S2/S3.



Auto-login username: admin

Terminal-type string: xterm

Terminal speeds: 38400,38400

Bild 28: PuTTY: Specifying the user name for automatically logging into the iRMC S2/S3

Configuring the OpenSSH client program ssh for using the public SSHv2 key

You establish an SSHv2-protected connection to the iRMC S2/S3 using the OpenSSH client program *ssh*. You can log in either under your current local login or under a different login.

The login must have been configured as a local login on the iRMC S2/S3 and the associated SSHv2 key must have been loaded on the iRMC S2/S3.

ssh reads its configuration options in order from the following sources:

1. Command line arguments that you specify when calling *ssh*:
2. User-specific configuration file (*$HOME/.ssh/config*)

i Although this file contains no security-critical information, read/write permission should only be granted to the owner. Access should be denied to all other users.

3. System-wide configuration file (*/etc/ssh/ssh_config*)

   This file contains default values for configuration parameters

   - if there is no user-specific configuration file or
   - if the relevant parameters are not specified in the user-specific configuration file.

The value found first applies for each option.

i You will find detailed information on the configuration of *ssh* and on its operands on the manual pages for OpenSSH under

http://www.openssh.org/manual.html

Proceed as follows:

► Start *ssh*, to log in to the iRMC S2/S3 under SSHv2-authentication:

```
ssh -l [<user>] <iRMC_S2/S3>
```

or

```
ssh [<user>@]<iRMC_S2/S3>
```

<user>
User name under which you want to log into the iRMC S2/S3. If you do not specify <user>, *ssh* uses the user name under which you are logged into your local computer to log you in to iRMC S2/S3.

<iRMC_S2/S3>
iRMC S2/S3 name or IP address of the iRMC S2/S3 you want to log into.

Example: SSHv2-authenticated login on the iRMC S2/S3

For the following *ssh*- call, it is assumed that *ssh-keygen* has been used to generate a public/private RSA key pair as described under "Example: Generating an RSA key pair with ssh -keygen" on page 75 and that the public key *User1/.ssh/id_rsa.pub* has been loaded onto the iRMC S2/S3 for an iRMC S2/S3 user *user4* (see page 77).

You can then log in from your local computer under *$HOME/User1* as follows on the iRMC S2 "RX100_S52-iRMC" using the login *user4*:

```
ssh user4@RX100_S52-iRMC
```

4.3.3.4 Example: Public SSHv2 key

The following shows the same public SSHv2 key in both RFC4716 format and in OpenSSH format.

Public SSHv2 key in RFC4716 format

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20090401"
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGsfc+F
pGJ2iw==
---- END SSH2 PUBLIC KEY ----
```

Public SSHv2 key in OpenSSH format

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGwsfc+F
pGJ2iw== rsa-key-20090401
```

5 Advanced Video Redirection (AVR)

ℹ A valid license key is required to use the Advanced Video Redirection function.

Advanced Video Redirection (AVR) allows you to control the mouse and keyboard of the managed server from your remote workstation and to show the current graphical and text output from the managed server.

ℹ The AVR Java applet allows you to use the Remote Storage function (see chapter "Remote Storage" on page 111).

This chapter provides information on the following topics:

- Checking the AVR settings
- Using AVR
- Menus of the AVR window

5.1 Requirements: Check the AVR settings

Check the following important settings before using AVR:

Graphics mode settings on the managed server

AVR supports the following graphics modes:

Resolution	Refresh rates [in Hz]	Maximum color depth [bits]
640 x 480 (VGA)	60; 75; 85	32
800 x 600 (SVGA)	56; 60; 72; 75; 85	32
1024 x 768 (XGA)	60; 70; 75; 85	32
1152 x 864	60; 70; 75	32
1280 x 1024 (UXGA)	60; 70; 75; 85	16
1280 x 1024 (UXGA)	60	24
1600 x 1200 (UXGA)	60; 65	16
1680 x 1050[1]	60	16
1920 x 1080[1]	60	16
1920 x 1200[1]	60	16

Table 3: Supported display settings

[1] iRMC S3 only

i If a high-resolution graphics mode is set on the server (shown on a gray background in the table), this is shown on the iRMC S2/S3 web interface.

i Only VESA-compliant graphics modes are supported.

Supported text mode

The iRMC S2/S3 supports the following common text modes:

- 40 x 25
- 80 x 25
- 80 x 43
- 80 x 50

Refer to the Help system for your operating system for information on the display settings.

Keyboard settings

i The keyboard settings must be identical:

- on the remote workstation,
- on the managed server,
- on the iRMC S2/S3.

5.2 Using AVR

► To start AVR, click the *Start Video Redirection* or *Start Video Redirection (Java Web Start)* button on the *Advanced Video Redirection (AVR)* page of the iRMC S2/S3 web interface (see page 302).

The *Advanced Video Redirection* window (AVR window) opens, showing you the display on the managed server.

The AVR window also contains the following elements:

- Menu bar: The *Preferences* and *Extras* menus allow you to configure the AVR settings and to control the AVR (see page 101). *Remote Storage* is used to call the remote storage function (see page 105). *Languages* (see page 107) menu allows you to set the language (German/English) in which the menus and dialog boxes of the AVR window are to be shown.
- Integrated special keys (see page 91).
- The *Local Monitor <status>* indicator shows whether the local monitor of the managed server is switched on (see section "Local Monitor Off" function" on page 90).

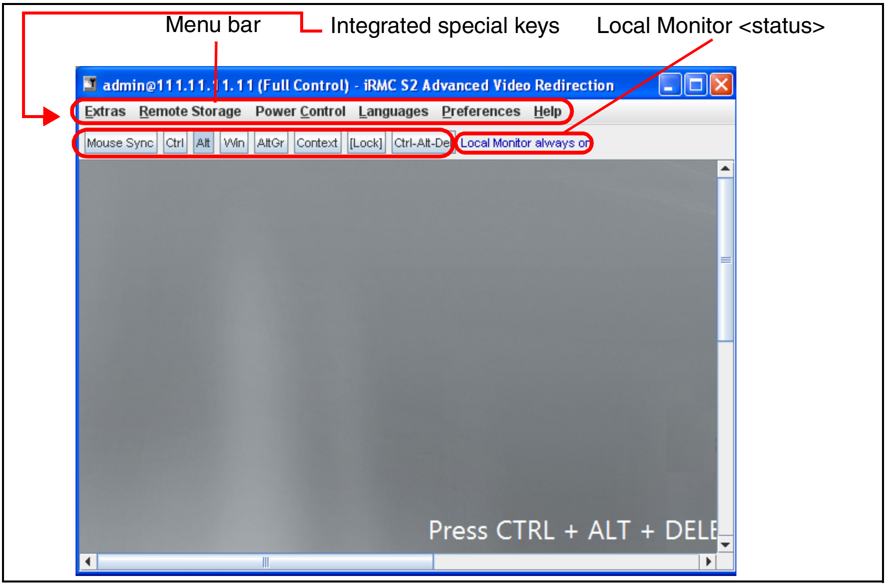


Figure 29: Advanced Video Redirection (AVR) window

5.2.1 Using a low bandwidth

In the case of a reduced data transfer rate, you can configure a lower bandwidth (bits per pixel, bpp) in terms of color depth for your current AVR session (see page 109).

5.2.2 Parallel AVR sessions

AVR can be used by two user sessions simultaneously. One user has full control over the server (full-control mode) and the other can only passively observe keyboard and mouse operation of the server (view only mode).

When AVR is first started, you are initially in view only mode. You will always be asked if you want to switch to full-control mode. If you decide to switch to full-control mode and another full-control mode session is already active, the existing session is switched to view-only mode.

5.2.3 Local Monitor Off" function

The *Local Monitor Off* function of the iRMC S2/S3 allows you to power down the local monitor of the managed server for the duration of your AVR session. In this way, you ensure that the inputs you make and the actions you perform on the local monitor on the server using AVR cannot be seen. The identification LED flashes to indicate "Local Monitor Off" mode on the server.

You configure the “Local Monitor Off” function on the *Advanced Video Redirection* page of the iRMC S2/S3 web interface (see page 302). After you have configured the system appropriately, you can switch the local monitor of the server on and off from the remote workstation as follows:

- In Full Control mode in an AVR session using the *Extras* menu
- directly on the *Advanced Video Redirection* page with administrator or OEM permissions

You can also configure that the local monitor is always switched off automatically whenever a new AVR session is started.

The current status of the local monitor is shown in the AVR window in blue letters to the top right of the integrated special keys:

The local monitor is always switched on and cannot be switched off, as the *Enable Local Monitor Off* option (see page 307) is deactivated.

Local Monitor On

The local monitor is on, but can be switched off.

Local Monitor Off

The local monitor is off, but can be switched on.

Local Monitor always off

The local monitor is always switched off and cannot be switched on because a high-resolution graphics mode has been set on the managed server (see table 3 on page 86).

5.2.4 Redirecting the keyboard

Keyboard redirection only works when the focus is on the AVR window.

- ▶ If keyboard redirection appears not to be working, simply click on the AVR window.
- ▶ If the keyboard does not respond, check that the AVR window is not in view-only mode. How to switch to full-control mode is described on page 103.

Special key combinations

AVR passes all normal key combinations to the server. Special keys such as Windows keys are not sent. Some special key combinations suchas [ALT] + [F4] cannot be sent, because they are interrupted by the client's operating system. In such cases, you should use the integrated special keys or the virtual keyboard.

Integrated special keys

Below the menu bar of the AVR window, you will find a bar containing the special keys. These keys are implemented as "sticky keys", i.e. they remain pressed when you click them and only return to their normal position when you click them again.

Using the integrated special keys, you can, for instance, use Windows keys or special key combinations which are not sent by AVR if you press them on your own keyboard.

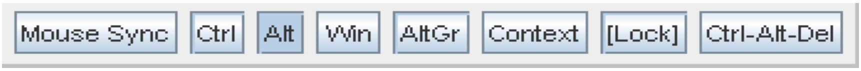


Figure 30: AVR window - integrated special keys

[Mouse Sync]

Press this key to synchronize the mouse pointers (see also section "Synchronizing the mouse pointer" on page 93).

[Ctrl]

Left CTRL key (corresponds to the [Ctrl] key on your keyboard).

[Alt]

Alt(ernate) key (corresponds to the [Alt] key on your keyboard).

[Win]

Left and right Windows keys (correspond to the keys on your keyboard between the left and right [Ctrl] and [Alt] keys).

[Alt Gr]

Alt(ernate) Gr(aphic) key (corresponds to the [Alt Gr] key on your keyboard).

[Context]

Context menu for the selected object (corresponds to the key combination [Shift] + [F10] on your keyboard).

[Lock]

Caps lock (corresponds to the [Caps Lock] key on your keyboard).

[Ctrl-Alt-Del]

Corresponds to the key combination [Ctrl]+ [Alt] + [Del] on your keyboard.

Virtual keyboard

The virtual keyboard (see figure 31) provides you with a functional representation of the keyboard. All key combinations are available when you use the virtual keyboard. This means that you can use the virtual keyboard as a fully functional replacement for a real keyboard.

You activate the virtual keyboard in the AVR window from the *Extras* menu (see page 102).

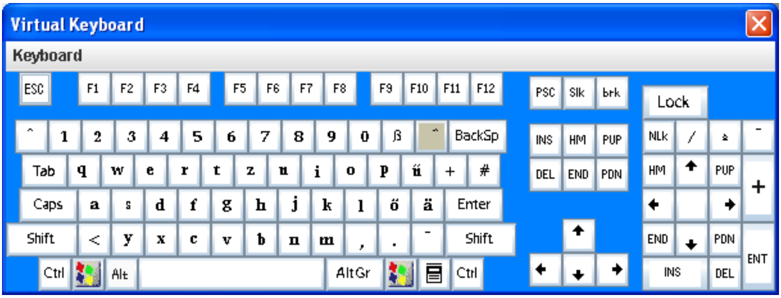

Virtual Keyboard
Keyboard
ESC F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 PSC Slk brk Lock
^ 1 2 3 4 5 6 7 8 9 0 ß ´ BackSp INS HM PUP NLk / * -
Tab q w e r t z u i o p ü + # DEL END PDN HM ↑ PUP +
Caps a s d f g h j k l ö ä Enter ← →
Shift < y x c v b n m , . - Shift ↑ END ↓ PDN ENT
Ctrl Alt AltGr Ctrl ← ↓ → INS DEL

Figure 31: Virtual Keyboard (keyboard layout: German (DE))

Secure Keyboard

If you are connected to the iRMC S2/S3 web interface over an HTTPS connection, entries at the keyboard are transferred over a secure SSL connection.

5.2.5 Redirecting the mouse

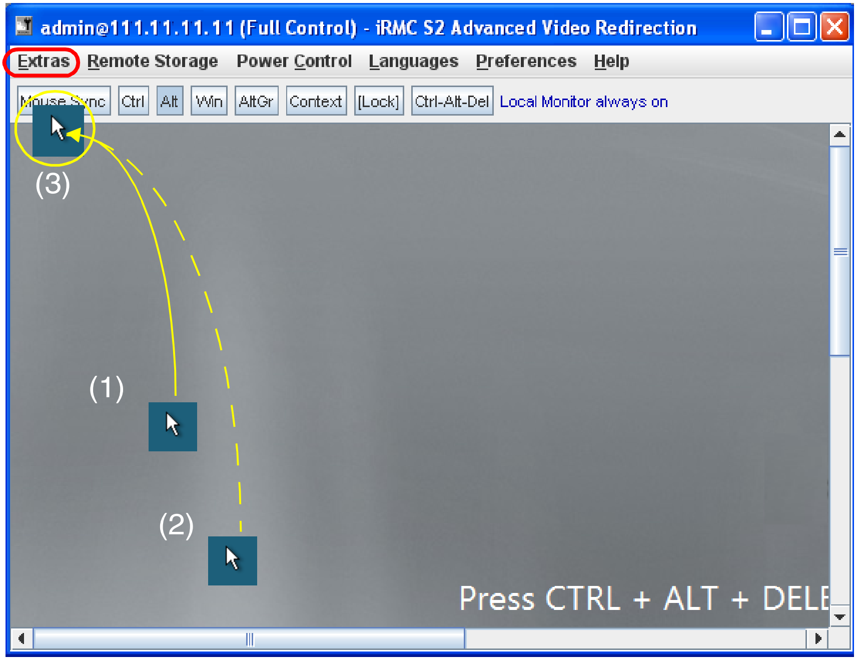
The mouse pointer on the managed server is moved synchronously with the mouse on the remote workstation. You configure the mouse redirection settings in the AVR window under *Mouse Mode* in the *Preferences* menu (see page 108).

5.2.5.1 Synchronizing the mouse pointer

When the AVR window is first opened, it is possible that the mouse pointer on the remote workstation (local mouse pointer) is not yet synchronized with the mouse pointer on the managed server.

To synchronize the two mouse pointers, use one of the following alternatives (see figure 32 on page 94):

- Click [Mouse Sync] in the menu bar of the AVR window.
- Move the local mouse pointer to the top left corner of the AVR window. The mouse pointer on the managed server automatically follows this movement. The pointers are synchronized when the two mouse pointers completely overlap.



Press the Mouse Sync key

or

(1) Drag the local mouse cursor to the top left corner.

(2) The server’s mouse pointer follows automatically.

(3) The mouse pointers are synchronized when they completely overlap and e displayed as **a single** mouse pointer.

Figure 32: Synchronizing the local mouse pointer and the mouse pointer of the managed server

i Correct synchronization of the mouse pointers requires that certain settings are made on the managed server. If the managed server has been installed using the ServerView Installation Manager these settings has been preconfigured automatically by the Matrox VGA installation.

If synchronization of the mouse pointers does not function correctly, for instance because the preconfigured settings have been changed, you can restore correct synchronization of the mouse pointers by making the settings described below. The settings must be made on the managed server.

ℹ The settings for the mouse pointer synchronization are supported only for the operating system which runs the managed server.

If the software which controls the mouse is active, sometimes the mouse pointer cannot be synchronized.

5.2.5.2 Managed Windows server: Adjusting the settings for synchronization of the mouse pointers

On a Windows server, you can either make the settings for mouse pointer synchronization using a batch program or using the Windows Start menu and the context menu.

You must adjust the following settings:

- Speed of the mouse pointer
- Hardware acceleration

ℹ When you adjust the settings using a batch program, the Matrox graphics driver is installed as well as the mouse pointer speed and hardware acceleration being adjusted.

You can make all the settings for the managed server either directly at the managed server or from the remote workstation over AVR.

Adjusting the settings on the managed server using a batch program

Proceed as follows:

► Open a DOS prompt window.

► Switch to the folder in which the batch program *install_kronos2_vga.bat* for the relevant Matrox VGA driver installation (32-bit or 64-bit) is located.

ℹ By default, you will find the *install_kronos2_vga.bat* programs under:

C:\Program Files\Fujitsu\ServerView Suite\Installation Manager\Content\V10.09.12.00\DRV\VIDEO\MATROX\iRMC\W2K

and on your ServerView Suite DVD 1.

► Type *setup.bat* to start the batch program.

► Reboot the managed server when the batch program has executed.

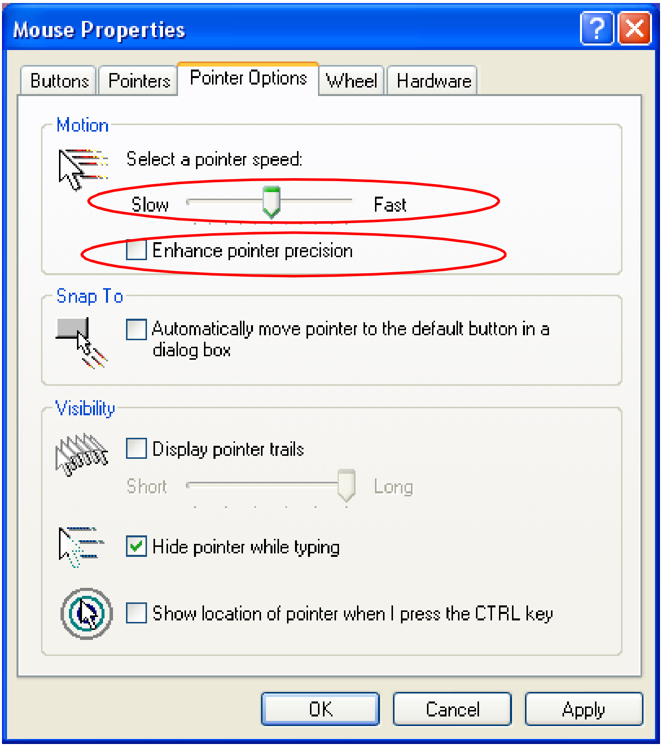
Adjusting the settings on the managed server using the Windows Start menu and the context menu

Proceed as follows to adjust the mouse pointer:

► Choose

Start - Settings - Control Panel - Printers and Other Hardware - Mouse and choose the *Pointer Options* tab.

This opens the following window:



Mouse Properties

Motion

Select a pointer speed:

Slow — Fast

□ Enhance pointer precision

Snap To

□ Automatically move pointer to the default button in a dialog box

Visibility

□ Display pointer trails

Short — Long

☑ Hide pointer while typing

□ Show location of pointer when I press the CTRL key

Figure 33: Mouse Properties - Pointer Options

► Set the *Pointer Speed* to a medium value.

► Disable the *Enhance Pointer Precision* option.

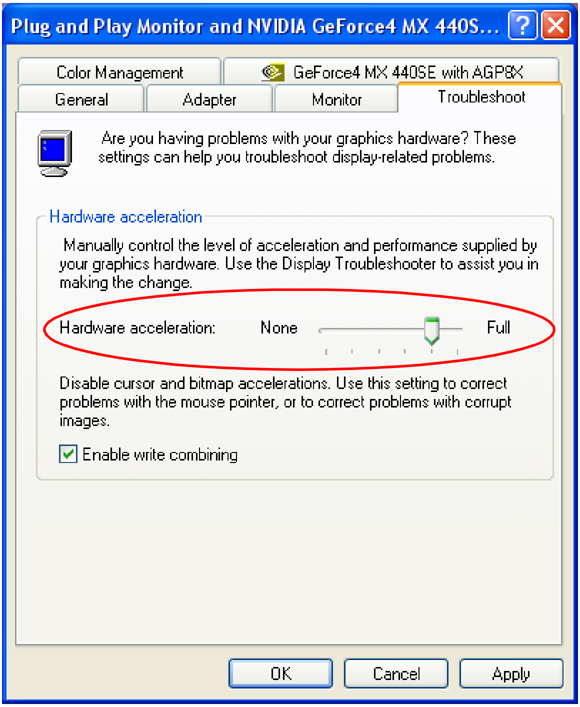
► Click the [OK] button to save the settings.

Proceed as follows to adjust the hardware acceleration:

- ► Right-click on the desktop background.
- ► In the context menu that appears, choose:

  Properties - Settings tab, *Advanced* button, and the *Troubleshooting* tab.

  This opens the following window:


Plug and Play Monitor and NVIDIA GeForce4 MX 440S...
Color Management
GeForce4 MX 440SE with AGP8X
General
Adapter
Monitor
Troubleshoot
OK
Cancel
Apply

Are you having problems with your graphics hardware? These settings can help you troubleshoot display-related problems.

Hardware acceleration

Manually control the level of acceleration and performance supplied by your graphics hardware. Use the Display Troubleshooter to assist you in making the change.

Hardware acceleration: None Full

Disable cursor and bitmap accelerations. Use this setting to correct problems with the mouse pointer, or to correct problems with corrupt images.

☑ Enable write combining

Figure 34: Properties - ... - Troubleshooting: Hardware acceleration

- ► Set the *Hardware Acceleration* to a value as shown in figure 34.
- ► Click the OK button to save the settings.

5.2.5.3 Managed Linux server: Adjusting the settings for synchronization of the mouse pointers

Prerequisite: The managed server is running under one of the following Linux operating systems:

- Red Hat 4.x
- Red Hat 5.x
- Suse 9.x
- Suse 10.x
- Suse 11.x

Different graphical user interfaces (GUIs) are available for Suse Linux and Redhat Linux. The most important GUIs are:

- Gnome
- KDE

You can adjust the mouse pointer synchronization settings on the managed server either using commands or under menu guidance.

You must adjust the following settings:

- *Mouse motion acceleration* = 1
- *Mouse motion threshold* =1

You can make all the settings for the managed server either directly at the managed server or from the remote workstation over AVR.

Adjusting temporary settings on the managed server using commands

Use the *xset* command to make the settings for *Pointer acceleration* and *Pointer threshold* (recommended values: 1 in each case) for the duration of the current session.

Command syntax:

```
xset m(ouse)][acceleration][threshold]
```

Proceed as follows:

- ► Call a command line tool.
- ► Run the command *xset* with the following arguments:

```
xset m 1 1
```

Adjusting permanent settings on the managed server using a configuration file (KDE)

You make permanent settings as follows for **KDE**:

- Change the settings in the text file */root/.kde/share/config/kcminputrc* as follows:

```
[Mouse]
Acceleration=1
Threshold=1
```

i It is not necessary to set the values again after rebooting the server.

Adjusting the permanent settings on the managed server under menu guidance

i It is not necessary to set the values again after rebooting the server.

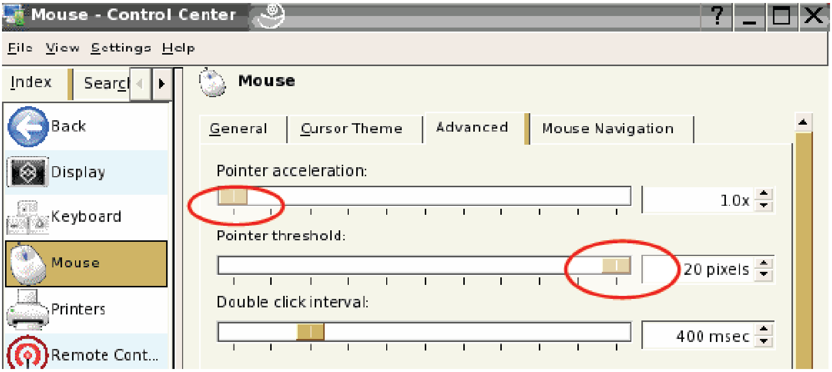
You make permanent settings as follows for **KDE**:

i The procedure for KDE described below only applies to Suse Linux.

- Choose

  N - Control Center - Peripheral - Mouse - Advanced tab

  The *Mouse - Control Center* window opens:



Pointer acceleration: 1.0x

Pointer threshold: 20 pixels

Double click interval: 400 msec

Figure 35: Mouse Control Center window

- ► Set the following values in the *Mouse Control Center* window:
  - – *Pointer acceleration:* 1.0x (minimum value)
  - – *Pointer threshold:* 20 pixels (maximum value)
- ► Save the settings.
- ► Reboot the managed server.

  i It is not necessary to set the values again after rebooting the server.

You make permanent settings as follows for **Gnome**:

- ► Call the *gconf-editor* editor under the shell.
- ► Choose: *desktop - gnome - peripherals - mouse*
- ► Modify the following attribute values:

  motion_acceleration 1
  motion_threshold 1

5.3 Menus of the AVR window

The menu bar of the AVR window contains the following menus:

- The *Extras* menu allows you to control the AVR session. You can also make a virtual keyboard available.
- You can set up and clear remote storage connections with the *Remote Storage* menu.
- The *Power Control* menu allows you to power the server up/down or to reboot the server.
- The *Languages* menu allows you to set the language (German/English) used to display the AVR menus and dialogs.
- The *Preferences* menu allows you to configure the mouse, keyboard and logging settings.

5.3.1 Extras menu

You can select the following functions in the *Extras* menu:

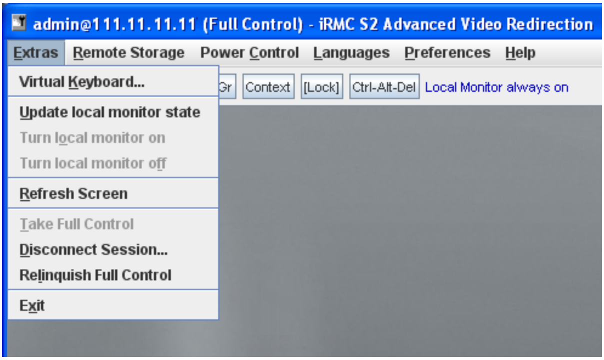


Figure 36: AVR window - Extras menu

Virtual Keyboard ...

The *Virtual Keyboard* window opens (see figure 31 on page 92).

Update local monitor state

Refreshes the display of the local monitor state.

Turn local monitor on

Switches on the local monitor of the managed server.

This function is disabled in the following cases, even if the local monitor is switched off:

– you are in view-only mode,

– A high-resolution graphics mode is set on the managed server (see table 3 on page 86).
Local monitor <status> display:
Local Monitor always off

Turn local monitor off

Switches off the local monitor of the managed server.

i This function is disabled in the following cases, even if the local monitor is switched on:

- you are in view-only mode,
- When AVR was started, the *Local Monitor Off* option was not enabled under *Local Monitor* (see page 306).
  Local monitor <status> display:
  Local Monitor always on

Refresh Screen

Refreshes the AVR window.

Take Full Control...

Switch to full-control mode. (This function is disabled if you are already in full-control mode.)

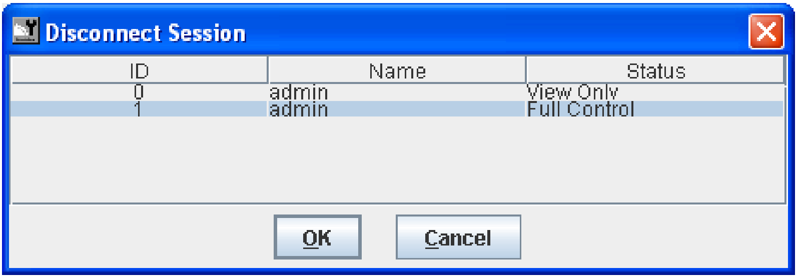
i An already existing full-control session will be notified by the notified. If the currently existing full-control session refuses your attempt to take full control, your session will remain in view-only mode.

Disconnect Session...

Terminate another AVR session.

i It is only possible to terminate other AVR sessions with *Disconnect Session*. To terminate your own session, choose *Exit*.

A list of current AVR sessions appears:



Disconnect Session

ID	Name	Status
0	admin	View Only
1	admin	Full Control

Figure 37: Extras menu - Disconnect Session

- ▶ Select the AVR session that you wish to terminate.
- ▶ Click *OK* to confirm that you want to terminate the selected AVR session.
- ▶ Click *Cancel* if you do not want to terminate the selected AVR session.

Relinquish Full Control...

Switch to view-only mode. (This function is disabled if you are already in view-only mode.)

Exit

Terminate your own AVR session.

5.3.2 Remote Storage menu

You call the remote storage functionality under *Remote Storage*:

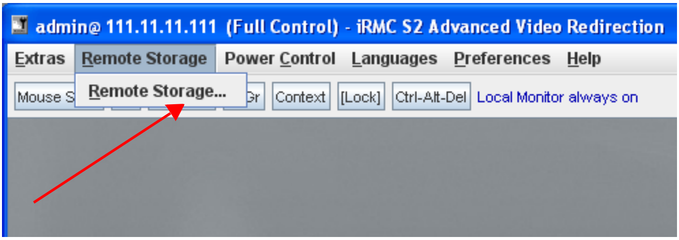


Figure 38: AVR window - Remote Storage menu

Remote Storage...

Click *Remote Storage...* to open the *Storage Devices* window (see page 115). This window allows you to attach or detach media on the remote workstation as Remote Storage devices (see chapter "Remote Storage" on page 111).

5.3.3 Power Control menu

The *Power Control* menu allows you to power the server up/down or to reboot the server:

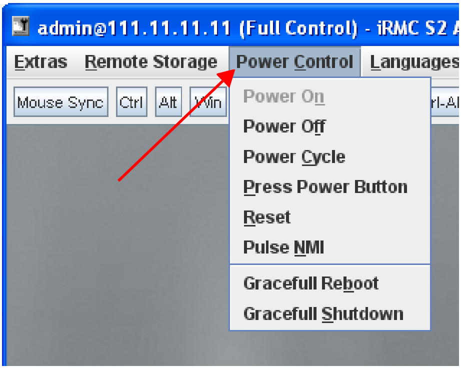


Figure 39: AVR window - Power Control menu

Power On

Switches the server on.

Power Off

Powers the server down, regardless of the status of the operating system.

Power Cycle

Powers the server down completely and then powers it up again after a configured period. You can configure this time in the *Power Cycle Delay* field of the *ASR&R Options* group (see page 234).

Press Power Button

Depending on the operating system installed and the action configured, you can trigger various actions by briefly pressing the power-off button. These actions could be shutting down the computer or switching it to standby mode or sleep mode.

Reset

Completely restarts the server (cold start), regardless of the status of the operating system.

Pulse NMI

Initiates a non-maskable interrupt (NMI). A NMI is a processor interrupt that cannot be ignored by standard interrupt masking techniques in the system.

Graceful Reboot

Graceful shutdown and reboot.
This option is only available if ServerView agents are installed and signed onto the iRMC S2/S3 as “Connected”.

Graceful Shutdown

Graceful shutdown and power off.
This option is only available if ServerView agents are installed and signed onto the iRMC S2/S3 as “Connected”.

5.3.4 Languages menu

From the *Languages* menu, choose the language in which the menus and dialog boxes of the AVR window are to be shown:

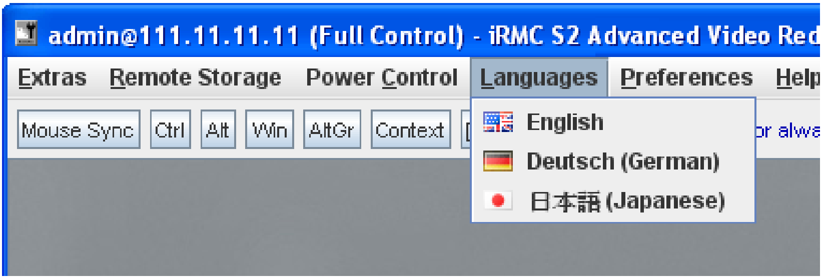
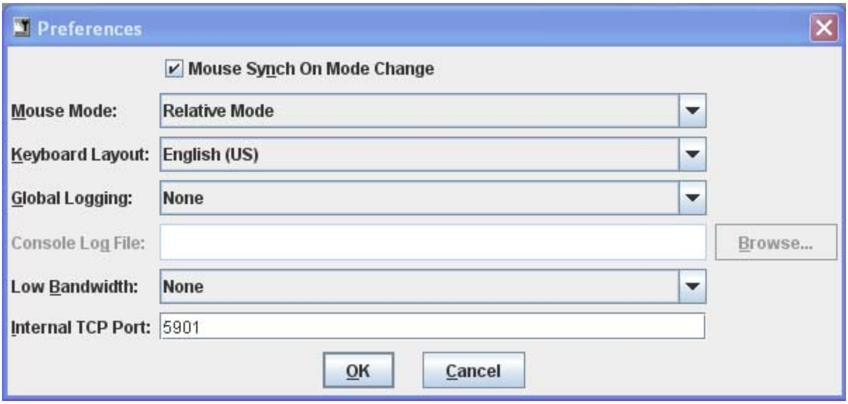


Figure 40: AVR window - Languages menu

5.3.5 Preferences menu

The *Preferences* menu allows you to configure the mouse mode, keyboard layout, global logging, low bandwidth, and the internal TCP port:



☑ Mouse Synch On Mode Change

Mouse Mode: Relative Mode

Keyboard Layout: English (US)

Global Logging: None

Console Log File:

Low Bandwidth: None

Internal TCP Port: 5901

Figure 41: AVR window - Preferences menu

If Video Redirection is executed in the *Num Lock On* mode on the server side, the client side also turns to *Num Lock ON*.

Mouse Synch On Mode Change

Default: Enabled.
Specifies whether or not mouse pointer synchronization should be kept up after changing the Mouse Mode (see below).

Mouse Mode

Specifies the mouse mode (*Hide Mode (Relative)*, *Absolute Mode* or *Relative Mode*).

Depending on the server operating system, you must make the following settings:

– Windows: *Absolute Mode*, *Hide Mode (Relative)* or *Relative Mode*
– Linux: *Hide Mode (Relative) or Relative Mode*

Default setting: *Absolute Mode*

Keyboard Layout

Specifies the keyboard layout for the virtual console.

> The keyboard layout at the managed server must also be set accordingly, i.e. the keyboard layout settings of AVR client and AVR server must be identical.

Global Logging

Default: No global logging.
Specifies whether global logging is to be carried out.

> Global logging must be disabled, i.e. *None* must be set!

Console Log File

Specifies the log file for global logging.

> Depending on your selection under *Global Logging,* this option may be disabled.

Low Bandwidth

In the case of a reduced data transfer rate, you can configure here a lower bandwidth (bits per pixel, bpp) in terms of color depth for your all AVR sessions at the same iRMC S2/S3.

None

Default.
No lower bandwidth.

3 bpp

3 bpp color depth (8 colors).

8 bpp

8 bpp color depth (256 colors).

Internal TCP Port

Default: 5901
Specifies the internal TCP port for the integrated Remote Storage Client used at the AVR Client.

6 Remote Storage

i A valid license key is required to use the Remote Storage function.

Remote Storage makes available to the managed server a “virtual” drive which is located elsewhere in the network. Up to two media can be redirected.

You can provide the source for the virtual drive as follows:

– Via a remote storage connection as a physical drive or image file at the remote workstation using the AVR Java applet (see page 113) via a remote connection:

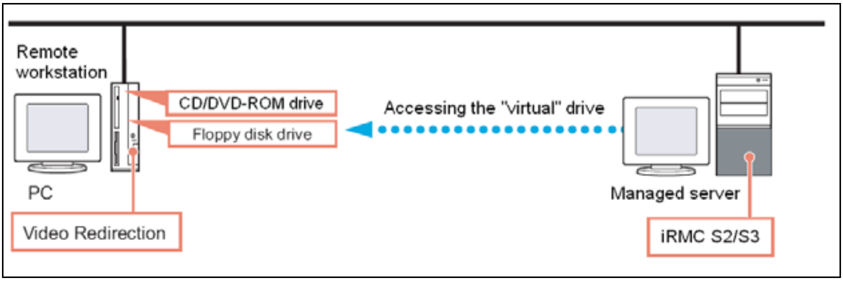


Figure 42: Remote storage via a remote connection

– As a CD/DVD ISO image file centrally in the network via a Remote Storage server (see page 127):

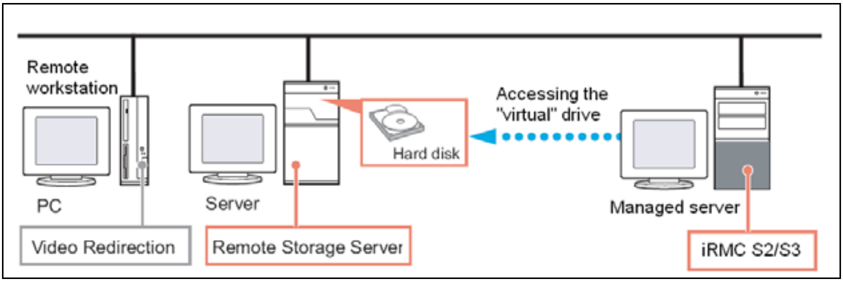


Figure 43: Remote storage via a Remote Storage Server

Parallel remote storage connections:

The following are possible concurrently:

- **either up to two** Remote Storage connections to virtual drives at the remote workstation (if the connection is established over the AVR Java applet)

  or

- **one** Remote Storage connection to a Remote Storage server.

It is not possible to establish concurrent Remote Storage connections via an applet and via the Remote Storage server.

The *Remote Storage* page of the iRMC S2/S3 web interface allows you to obtain information on the status of the current remote storage connections and establish the connection to a Remote Storage server (see page 312).

6.1 Providing remote storage at the remote workstation

If you provide the source for a virtual drive on the remote workstation then the remote storage functionality supports the following device types:

- Floppy
- CD ISO image
- DVD ISO image
- CD, DVD

i Optical storage media (CD, DVD) are automatically displayed (offered for selection). Other remote storage media must be made available as remote storage by manually selecting the appropriate device type.

i Devices connected as remote storage are recognized as the USB connected devices by the iRMC S2/S3. They cannot be used if no USB connection is available (e.g. no USB driver exists).

You can use the virtual drive to install an operating system on your PRIMERGY server from the remote workstation (see chapter "Remote installation of the operating system via iRMC S2/S3" on page 371).

This section provides information on the following topics:

- Starting Remote Storage
- Provision of storage media for Remote Storage
- Connecting storage media as remote storage
- Clearing Remote Storage connections
- Removing media made available for Remote Storage

6.1.1 Starting Remote Storage

You start the Remote Storage function using the AVR Java applet (see section "Advanced Video Redirection - Start Advanced Video Redirection (AVR)" on page 302).

- ► Start the iRMC S2/S3 web interface (see section "Logging into the iRMC S2/S3 web interface" on page 136).
- ► Open the *Advanced Video Redirection* page and click on the *Start Video Redirection,* button to start Advanced Video Redirection (see section "Advanced Video Redirection - Start Advanced Video Redirection (AVR)" on page 302).

  This opens the AVR window.
- ► In the menu bar in the AVR window, choose: *Remote Storage - Remote Storage...*

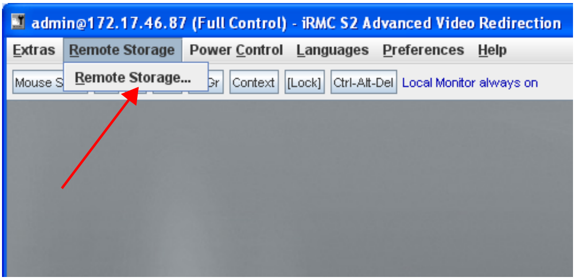


Figure 44: AVR window - Remote Storage - Remote Storage...

The *Storage Devices* dialog box opens, containing the storage media currently available for Remote Storage.

“Storage Devices” dialog box on a Windows system

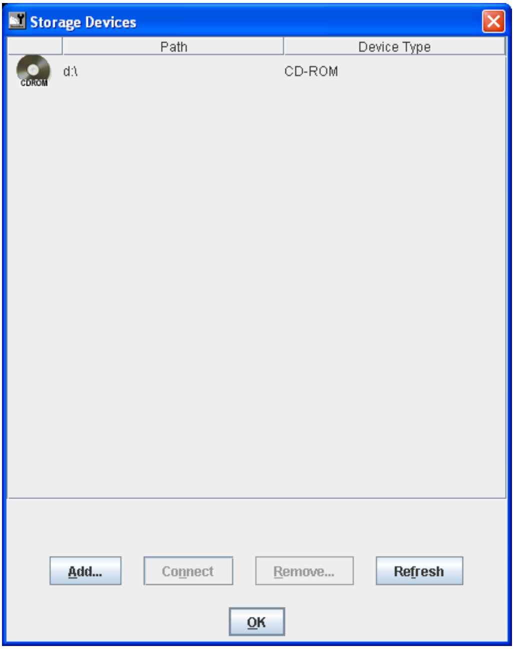


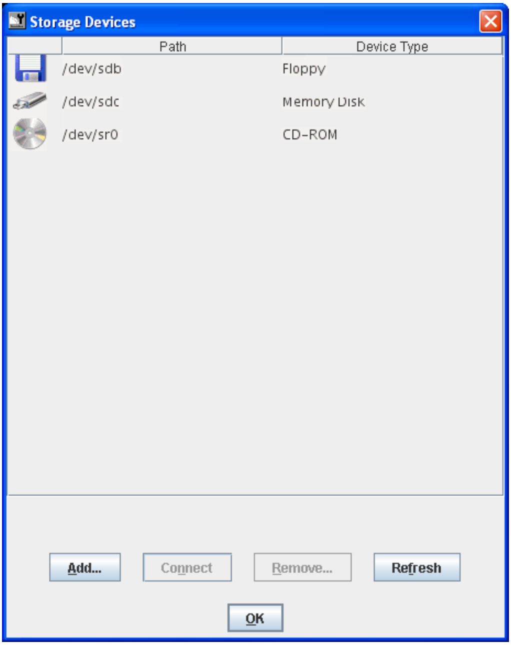
Figure 45: Storage Devices dialog box

i When a storage medium is inserted in an optical drive (CD ROM, DVD ROM) the contents are displayed automatically.

Floppy disk drives and CD ROM / DVD ROM drives are not displayed in the list unless a medium is inserted.

If a storage medium is inserted, but its contents are not displayed, the storage medium is reserved by the local explorer.

“Storage Devices” dialog box on a Linux system



Storage Devices

Path	Device Type
/dev/sdb	Floppy
/dev/sdc	Memory Disk
/dev/sr0	CD-ROM

Figure 46: Storage Devices dialog box

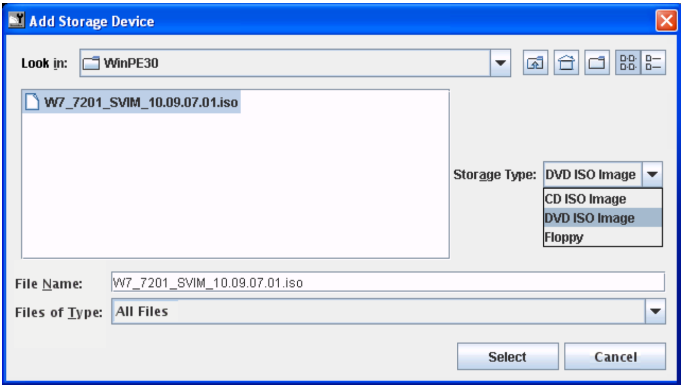
Physical storage media must be mounted to allow them to be connected as Remote Storage devices. Mounted storage media are automatically displayed in the *Storage Devices* dialog box.

6.1.2 Provision of storage media for emote Storage

► In the *Storage Devices* dialog box, click *Add...* .

The *Add Storage Device* dialog box opens.

“Add Storage Device” dialog box on a Windows system



Look in: WinPE30

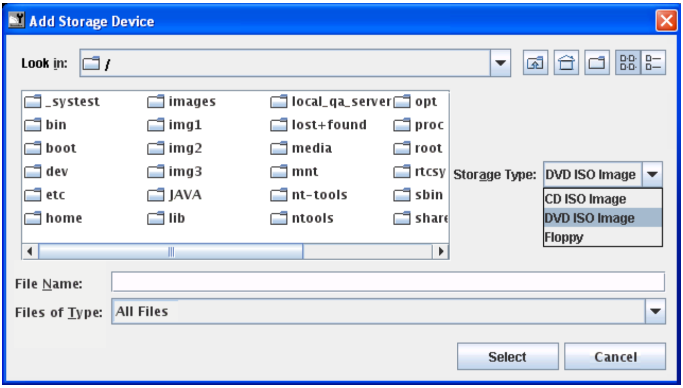
Storage Type: DVD ISO Image

File Name: W7_7201_SVIM_10.09.07.01.iso

Files of Type: All Files

Figure 47: Add Storage Device dialog box (Windows)

“Add Storage Device” dialog box on a Linux system



Look in: /

Storage Type: DVD ISO Image

File Name:

Files of Type: All Files

Figure 48: Add Storage Device dialog box (Linux)

► In the *Add Storage Device* dialog box, navigate to the directory of the remote storage medium that you want to make available for remote storage from your remote workstation.

► Select the required device type under *Storage Type*.

The following storage types can be selected:

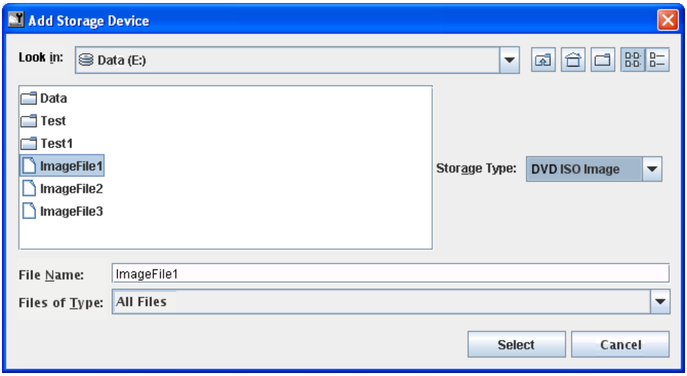
- Floppy
- CD ISO image
- DVD ISO image

i Physical storage devices must be mounted on Linux systems.

► Specify the storage medium you wish to connect as Remote Storage under *File Name*:

- In the case of an ISO image (ISO/NRG image), enter the file name. Alternatively, click on the file name in the Explorer.
- In the case of a drive, enter the name of the drive, e.g.
  - “D” for drive D (Windows)
  - */dev/...* (Linux)

“Add Storage Device” dialog: Selecting the storage medium (Windows)



Look in: Data (E:)

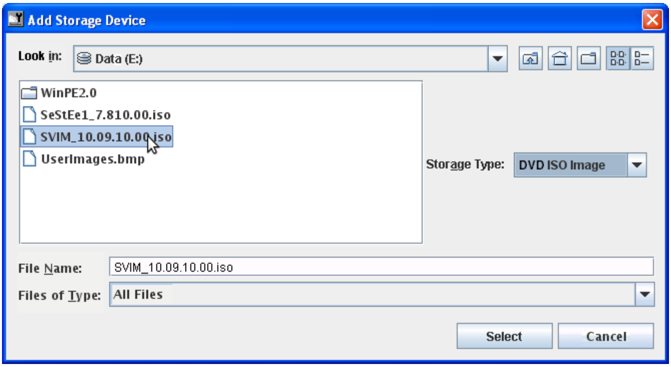
Storage Type: DVD ISO Image

File Name: ImageFile1

Files of Type: All Files

Figure 49: Add Storage Device dialog: Selecting the storage medium

"Add Storage Device" dialog: Selecting the storage medium (Linux)



Look in: Data (E:)

- WinPE2.0
- SeStEe1_7.810.00.iso
- SVIM_10.09.10.00.iso
- UserImages.bmp

Storage Type: DVD ISO Image

File Name: SVIM_10.09.10.00.iso

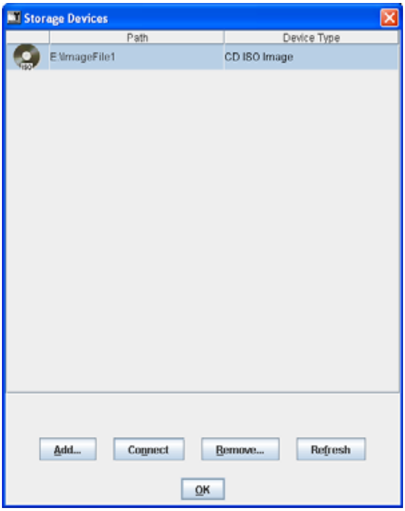
Files of Type: All Files

Figure 50: Add Storage Device dialog: Selecting the storage medium

► Click *Select* to confirm your selection.

The selected storage medium is made available for Remote Storage and displayed in the *Storage Devices* dialog.

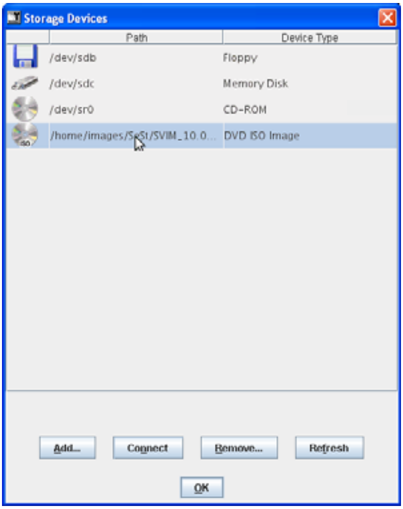
Display in the "Storage Devices" dialog (Windows)



Path	Device Type
E:\ImageFile1	CD ISO Image

Figure 51: Storage Devices dialog: The provided storage medium is displayed.

Display in the “Storage Devices” dialog (Linux)



	Path	Device Type
	/dev/sdb	Floppy
	/dev/sdc	Memory Disk
	/dev/sr0	CD-ROM
	/home/images/SeSt/SVIM_10.0...	DVD ISO Image

Figure 52: Storage Devices dialog: The provided storage medium is displayed.

6.1.3 Connecting storage media as remote storage

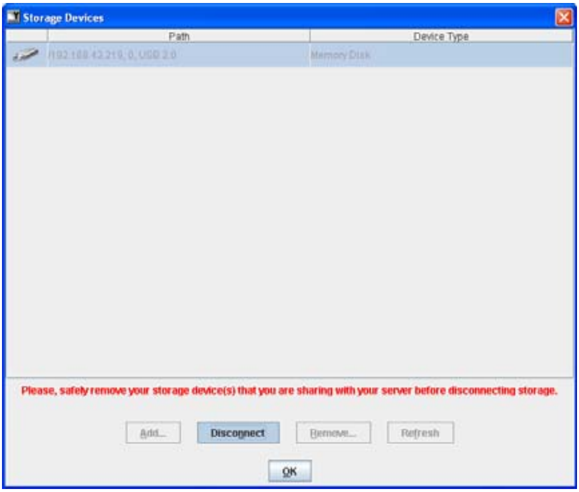
► In the *Storage Devices* dialog (see figure 51 and figure 52 on page 120), click the storage medium that you want to connect as Remote Storage.

► Click *Connect* to connect the selected storage medium as Remote Storage.

The *Storage Devices* dialog opens with the message regarding safe removal. The storage medium is connected as Remote Storage.

i If you wish to connect two storage devices as Remote Storage at the same time, a confirmation dialog box is displayed before the connection is established (see section "Connecting two storage devices as Remote Storage at the same time" on page 123).

Storage Devices dialog: Showing Remote Storage connection (Windows)



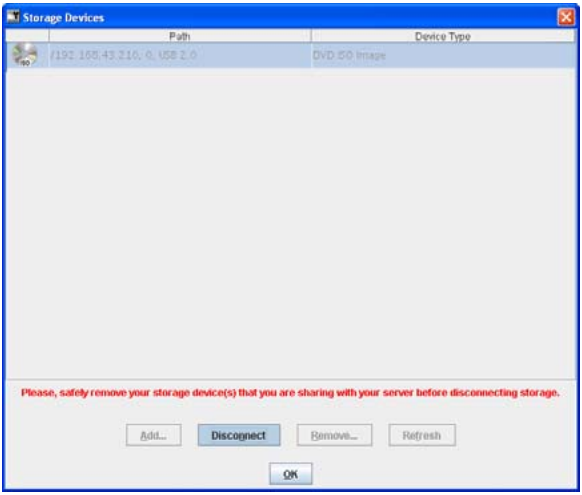
Storage Devices

	Path	Device Type
	/192.168.43.219, 0, USB 2.0	Memory Disk

Please, safely remove your storage device(s) that you are sharing with your server before disconnecting storage.

Figure 53: Storage Devices dialog: The storage medium is connected as Remote Storage.

Storage Devices dialog: Showing Remote Storage connection (Linux)



Path	Device Type
/192.168.43.210, 0, USB 2.0	DVD ISO Image

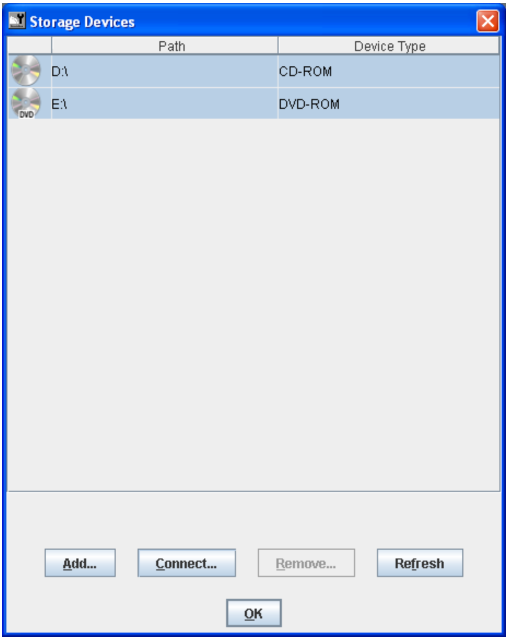
Please, safely remove your storage device(s) that you are sharing with your server before disconnecting storage.

Figure 54: Storage Devices dialog: The storage medium is connected as Remote Storage.

Connecting two storage devices as Remote Storage at the same time

The example in the following section illustrates how to simultaneously connect two storage media as Remote Storage on a Windows system. The same procedure applies for Linux systems.

In figure 55, you can see that two storage devices have been provided as Remote Storage:

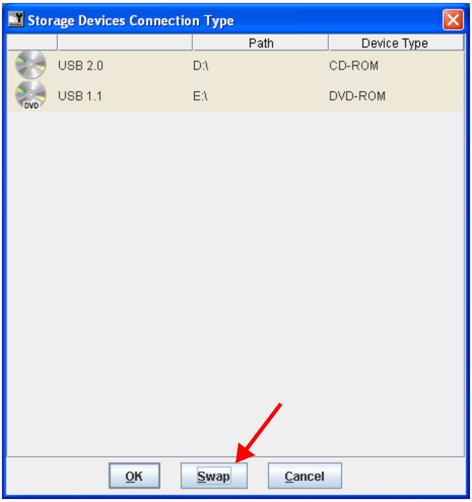


Path	Device Type
D:\	CD-ROM
E:\	DVD-ROM

Figure 55: Storage Devices dialog: Connecting 2 storage devices as Remote Storage

- ► Select the two storage devices and click *Connect* to connect the storage devices as Remote Storage.

  The system then makes a proposal regarding the assignment of your storage devices to USB 1.1 and USB 2.0 (see figure 55 on page 123).

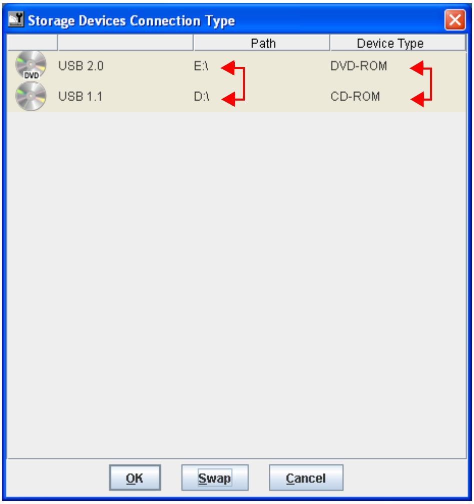


Storage Devices Connection Type

	Path	Device Type
USB 2.0	D:\	CD-ROM
USB 1.1	E:\	DVD-ROM

Figure 56: Connection Type dialog: Assignment to USB 1.1 and USB 2.0

- ► Click *Swap* if you want to swap the assignment of the storage devices to USB 1.1 and USB 2.0.



Storage Devices Connection Type

	Path	Device Type
USB 2.0	E:\	DVD-ROM
USB 1.1	D:\	CD-ROM

Figure 57: Connection Type dialog: Assignment to USB 1.1 and USB 2.0 swapped

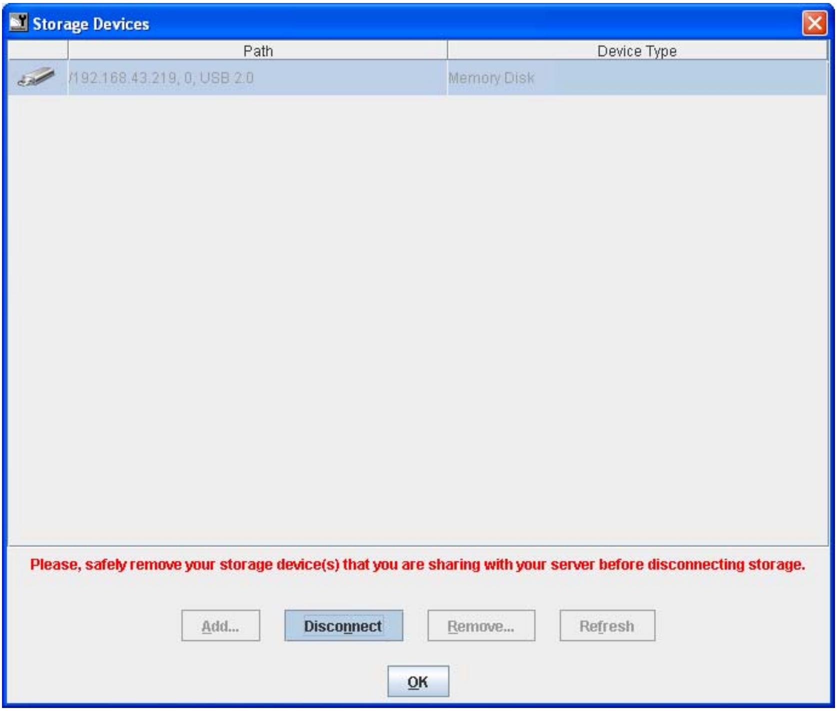
- ► Click *OK* to connect the storage devices as Remote Storage.

6.1.4 Clearing Remote Storage connections

The Remote Storage connection is automatically released when the AVR session is disconnected.

- Open the *Storage Devices* dialog (see section "Starting Remote Storage" on page 114).

  The list of storage media connected as Remote Storage is displayed (using Windows in the example).



Path	Device Type
/192.168.43.219, 0, USB 2.0	Memory Disk

Please, safely remove your storage device(s) that you are sharing with your server before disconnecting storage.

Figure 58: Storage Devices dialog: Clearing Remote Storage connections

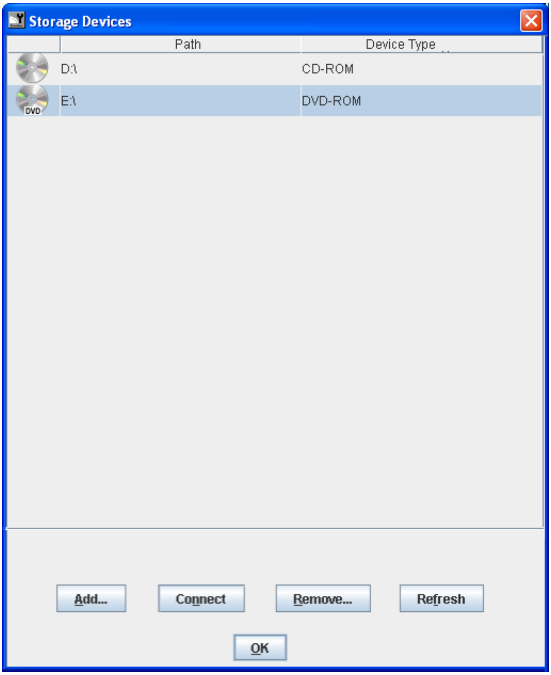
- “Safely remove” the storage device, i.e. ensure that no more applications/programs are accessing the storage media.
- Click *Disconnect* to clear all Remote Storage connections.

6.1.5 Removing the storage medium

Remove a storage medium from the list of media available for Remote Storage as follows:

- Open the *Storage Devices* dialog (see section "Starting Remote Storage" on page 114).

  The list of storage media available for Remote Storage is displayed (using Windows in the example):



Storage Devices

Path	Device Type
D:\	CD-ROM
E:\	DVD-ROM

Figure 59: Storage Devices dialog: Removing a Remote Storage medium

- Select the storage medium you want to remove.
- Click *Remove...* to remove the storage medium.

6.2 Providing remote storage via a Remote Storage server

You can use a Remote Storage server to provide an image file (ISO/NRG image) as remote storage for any number of PRIMERGY servers that can be administered via iRMC S2/S3. You can use this image file to boot one or more PRIMERGY servers from the remote workstation (see chapter "Remote installation of the operating system via iRMC S2/S3" on page 371).

The Remote Storage server is available for Windows systems

i The Remote Storage server is available in a 32-bit and 64-bit variant for Windows. The 32-bit and 64-bit versions of the Remote Storage server must not be installed at the same time on 64-bitsystems.

i You will find the individual variants of the Remote Storage server on your ServerView Suite DVD 1 under

SVSoftware\Software\RemoteView\iRMC

Making the ISO image available to the PRIMERGY Server via Remote Storage

The following requirements must be satisfied if your PRIMERGY server is to use the image file made available by the Remote Storage server:

- The Remote Storage server must be installed (see page 128).
- The Remote Storage server must be started (see page 133).
- The managed server’s iRMC S2/S3 must be connected to the Remote Storage server (see page 312).

Booting from WinPE 2.x-based ISO images

A PRIMERGY server running iRMC S2/S3 and a firmware version ≥ 3.60A is required to boot from a WinPE 2.x-based ISO image (e.g. Windows Server 2008 and ServerView Installation Manager).

6.2.1 Installing the Remote Storage server

The Remote Storage server is available in 32-bit and 64-bit versions. The 32-bit and 64-bit versions of the Remote Storage server must not be installed at the same time on 64-bit systems.

The installation programs *RemoteStorageServer_Installer32.exe* and *RemoteStorageServer_Installer64.exe* for installing the Remote Storage server are located on the ServerView Suite DVD 1 under *SVSoftware\Software\RemoteView\iRMC\Widows_32* and *SVSoftware\Software\RemoteView\iRMC\Widows_x64* respectively.

Once installation has been completed successfully, your installation directory contains a number of files including *RemoteStorageServer.exe*.

6.2.2 Remote Storage server execution modes

You can execute the Remote Storage server in the following modes as required:

- as a background service
- as a stand-along program

You configure the Remote Storage server execution mode via a graphical user interface (see page 130).

Executing the Remote Storage server as a service

The following points should be noted

- The image file can be located either on a computer in the network or on the same host on which the Remote Storage server is running.

  i If the image file is not on the computer on which the Remote Storage server is running, you must specify the path of the image file in UNC notation. You also need a user account with access permissions on the image file.

- When the host on which the Remote Storage server is located is booted, the remote storage server starts automatically. The Remote Storage server is then executed until it is explicitly terminated or the host is shut down.
- When the host on which the Remote Storage server is located is booted, the image file becomes available automatically.

Executing the Remote Storage server as a stand-alone program

The following points should be noted

- The image file (ISO/NRG image) may be present locally on the Remote Storage server or on an assigned network drive.
- When the host on which the Remote Storage server is located is booted, you must start the image file “manually”.

6.2.3 Configuring, starting and exiting the Remote Storage server

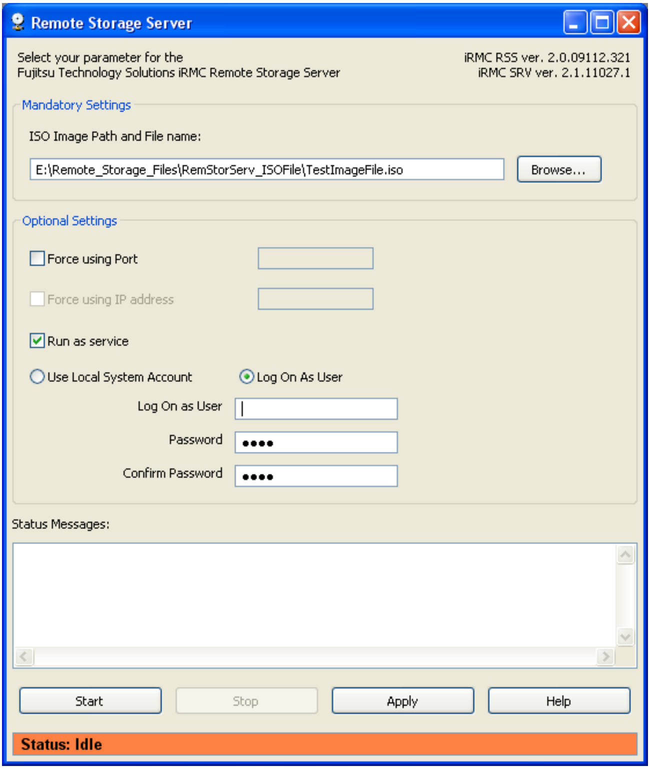
You configure, start and exit the Remote Storage server via a graphical user interface (GUI).

Calling the Remote Storage server’s raphical user interface

You call the Remote Storage server’s graphical user interface as follows:

- ► Choose *Start - Programs - Fujitsu RemoteStorageServer - Remote Storage Server*.

  The Remote Storage server’s graphical user interface appears:



Remote Storage Server

Select your parameter for the
Fujitsu Technology Solutions iRMC Remote Storage Server

iRMC RSS ver. 2.0.09112.321
iRMC SRV ver. 2.1.11027.1

Mandatory Settings

ISO Image Path and File name: E:\Remote_Storage_Files\RemStorServ_ISOFile\TestImageFile.iso

Optional Settings

□ Force using Port

□ Force using IP address

☑ Run as service

○ Use Local System Account ● Log On As User

Log On as User:

Password: ••••

Confirm Password: ••••

Status Messages:

Status: Idle

Figure 60: The Remote Storage server’s graphical user interface (here in the “Idle” state)

Configuring the Remote Storage server

i Configuration is only possible if the Remote Storage server is in the “idle” state, i.e. it is not being executed.

In the graphical user interface, you specify the image file made available as remote storage together with other parameters:

ISO Image Path and Filename:

► Enter the path and name of the image file directly in the field.

or:

► Click the *Browse...* button and then navigate to and select the required image file in the *Choose a file* dialog which now opens and then confirm.

i If the Remote Storage server is to run as a service (see the *Run as Service* option on page 132) and the image file is located on a computer in the network, you must specify the path of the image file in UNC notation. You must also ensure that the account entered under *Log On As User* (see page 132) is valid and has access permissions on the share on which the image file is located.

Force Using Port

If you have configured a port number other than the default port number (5901) for the iRMC S2/S3’s remote storage port (see page 248), then you must activate this option and enter the configured port number in the associated field.

Force Using IP Address

If the host on which the Remote Storage server is executed possesses more than one LAN connection:
You can specify the IP address of the LAN connection that is to be used for the Remote Storage server if this is executed as a service.
By default, the Remote Storage server uses the first detected LAN connection.

Run as Service

Activate this option if the Remote Storage server is to be executed as a service in the background (see page 129).

► Select one of the two options below:

Use Local System Account

The Remote Storage server is executed as a service under the local system account.

In this event, the image file (ISO/NRG image) must be located on a local drive.

Log On As User

he Remote Storage server is executed under the user account that you specify in the following input fields.

Specify the user name in the form:

– For local users: *.\Logon-Name*

– For domain users:

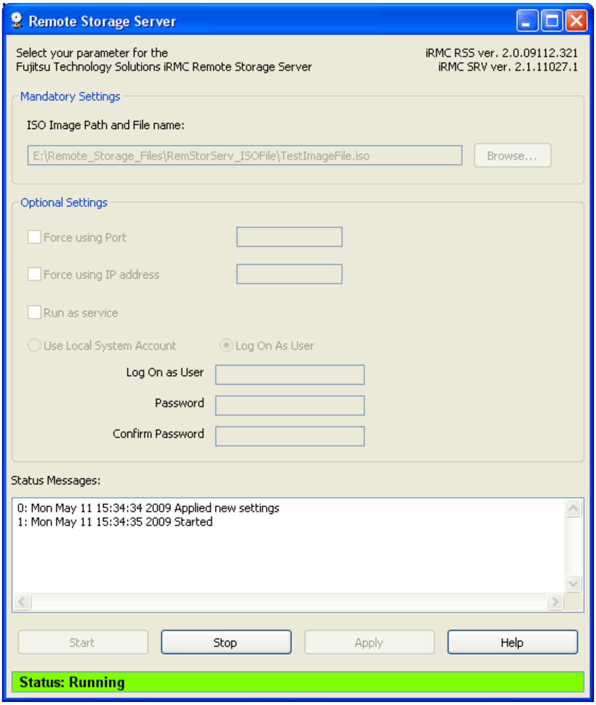
DOMAIN\LogOnName
or
LogOnName@DOMAIN<mailto:LogOnName@DOMAIN>

i The image file (ISO/NRG image) can be located on a network drive if the *Log On As User* option is enabled. In this event, the specified account must have access permissions on the network drive on which the image file is located. You must also specify the image file in UNC notation (see input field *ISO Image Path or Filename* on page 131).

► Click the *Apply* button to activate your settings.

Starting the Remote Storage server

► Click the *Start* button to start the Remote Storage server as a service or as a stand-alone program:



Remote Storage Server

Select your parameter for the
Fujitsu Technology Solutions iRMC Remote Storage Server

iRMC RSS ver. 2.0.09112.321
iRMC SRV ver. 2.1.11027.1

Mandatory Settings

ISO Image Path and File name: E:\Remote_Storage_Files\RemStorServ_ISOFile\TestImageFile.iso

Optional Settings

□ Force using Port

□ Force using IP address

□ Run as service

○ Use Local System Account ● Log On As User

Log On as User

Password

Confirm Password

Status Messages:

```
0: Mon May 11 15:34:34 2009 Applied new settings
1: Mon May 11 15:34:35 2009 Started
```

Status: Running

Figure 61: The Remote Storage server is executed (“Running” status)

Status Messages:

The logged execution states of the Remote Storage server are displayed here.

i If the *Run as service* execution mode is configured (see page 132), then the Remote Storage server is started automatically when the computer on which the Remote Storage server is installed is booted.

i Execution of the Remote Storage server is not interrupted automatically if the graphical user interface is exited.

Exiting the Remote Storage server

► Click the *Stop* button to terminate execution of the Remote Storage server.

7 iRMC S2/S3 web interface

The iRMC S2/S3 not only has its own operating system, but also acts as a web server, providing its own interface. You can choose whether to show the menus and dialog boxes of the iRMC S2/S3 web interface in German, English or Japanese.

When you enter values in the iRMC S2/S3 web interface, you often receive assistance in the form of tool tips.

i The software described below is based in part on the work of the Independent JPEG Group.

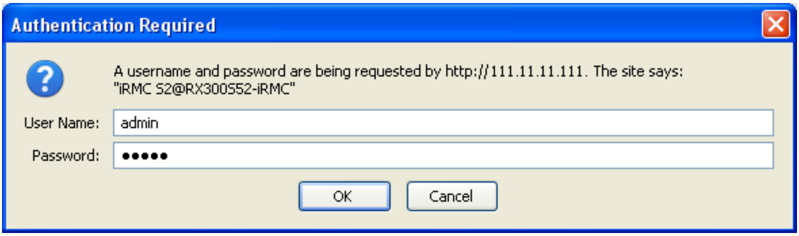
7.1 Logging into the iRMC S2/S3 web interface

- ► Open a web browser on the remote workstation and enter the (configured) DNS name (see page 249) or IP address of the iRMC S2/S3.

Different login screens appear depending on whether LDAP access to a directory service has been configured for the iRMC S2/S3 (*LDAP enabled* option, see page 274):

i If no login screen appears, check the LAN connection (see section "Testing the LAN interface" on page 47).

– LDAP access to the directory service is not configured for the iRMC S2/S3 (*LDAP enabled* option is not activated) and *Always use SSL Login* option (see page 274) is not activated:



A username and password are being requested by http://111.11.11.111. The site says: "iRMC S2@RX300S52-iRMC"

User Name: admin

Password: ●●●●●

Figure 62: Login screen for the iRMC S2/S3 web interface (LDAP access not configured and the “Always use SSL login” option is not selected)

► Type in the data for the default administrator account.

User name: admin

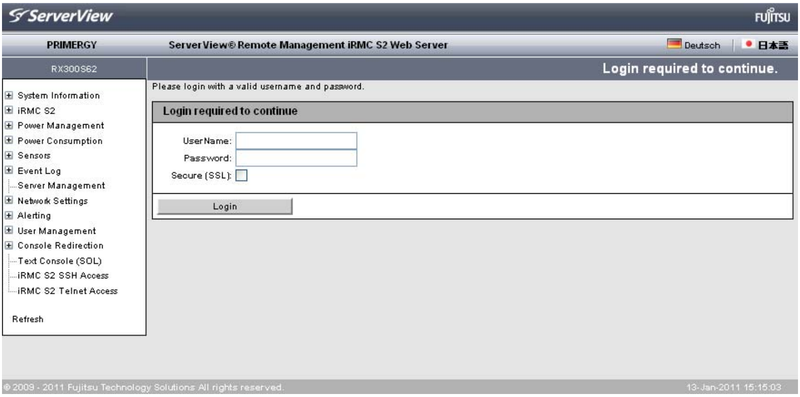
Password: admin

i Both the *User name* and the *Password* are case-sensitive.

For reasons of security, it is recommended that you create a new administrator account once you have logged in, and then delete the default administrator account or at least change the password for the account (see "User “<name>” Configuration - User configuration (details)" on page 266).

► Click *OK* to confirm your entries.

– LDAP access to the directory service is configured for the iRMC S2/S3 (*LDAP enabled* option is activated) or *Always use SSL Login* option is activated):



Login required to continue.

Please login with a valid username and password.

Login required to continue

User Name:

Password:

Secure (SSL): □

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.

13-Jan-2011 15:15:03

Figure 63: Login screen for the iRMC S2/S3 web interface (LDAP access configured)

> **i** The user name and password are always SSL-protected when they are transmitted. If you activate the *Secure (SSL)* option, all communication between the web browser and the iRMC S2/S3 is carried out over HTTPS.

► Type in the data for the default administrator account.

User name: admin

Password: admin

> **i** For reasons of security, it is recommended that you create a new administrator account once you have logged in, and then delete the default administrator account or at least change the password for the account (see "User “<name>” Configuration - User configuration (details)" on page 266).

► Click *Login* to confirm your entries.

The iRMC S2/S3 web interface opens showing the *System Information page* (see page 146).

7.2 Required user permissions

table 4 provides an overview of the permissions which are required in order to use the individual functions available at the iRMC S2/S3 web interface.

Functions in the iRMC S2/S3 web interface	Permitted with IPMI privilege level				Required iRMC S2/S3-specific permission			
	OEM	Administrator	Operator	User	Configure User Accounts	Configure iRMC S2/S3 Settings	Video Redirection Enabled	Remote Storage Enabled
Open the *System Overview* page.	X	X	X	X				
Switch identification LED on/off.	X	X	X	X				
Set *Asset Tag Configuration*.						X		
Edit *Operating System Informations*[1]						X		
Open the *System Component Information* page.	X	X	X	X				
Reset Memory Error Counter.						X		
View SPD Data.	X	X	X	X				
Open the *Backup/Restoration of BIOS Single Parameter Settings* page.[2]	X	X	X	X				
Edit *Backup/Restoration of BIOS Single Param. Settings*[2]	X	X						
Open the *BIOS Update Settings* page.[2]	X	X	X	X				
Perform BIOS update [2]	X	X				X		
Open the *iRMC S2/S3 Information* page.	X	X	X	X				
Reboot iRMC S2/S3.	X	X						
Load license key onto the iRMC S2/S3.						X		
Set *Miscellaneous Options*						X		
Open the *Save iRMC S2/S3 FW Settings* page.					X	X		

Table 4: Permissions to use special the iRMC S2/S3 web interface

Functions in the iRMC S2/S3 web interface	**Permitted with IPMI privilege level**				**Required iRMC S2/S3-specific permission**			
	OEM	**Administrator**	**Operator**	**User**	**Configure User Accounts**	**Configure iRMC S2/S3 Settings**	**Video Redirection Enabled**	**Remote Storage Enabled**
Select *Include User Settings*.					X			
Select any other setting option(s).						X		
Import iRMC S2/S3 settings in WinSCU XML format from file.					X	X		
Open/edit the *Certificate Upload* page.						X		
Open/edit the *Generate a self-signed RSA Cert.* page						X		
Open *iRMC S2/S3 Firmware Update* page.	X	X	X	X				
Set firmware selector.	X	X						
Perform *Firmware Update from File*.						X		
Update firmware via TFTP (*iRMC S2/S3 TFTP Settings*).						X		
Open *Power On/Off* page.	X	X	X	X				
Modify *Boot Options*.						X		
Use *Power Control*.	X	X	X					
Open/edit the *Power Options* page.						X		
Open *Power Supply Info* page.	X	X	X	X				
Open/edit *Power Consumption Configuration* page						X		
Open *Current Power Consumption* page[2)]						X		
Open/edit *Power Consumption History* page[2)].						X		
Open *Fans* page.	X	X	X	X				
Start fan test (*Fan Test* group).	X	X	X	X				
Set *Fan Check Time* (*Fan Test* group).						X		

Table 4: Permissions to use special the iRMC S2/S3 web interface

Functions in the iRMC S2/S3 web interface	Permitted with IPMI privilege level				Required iRMC S2/S3-specific permission			
	OEM	Administrator	Operator	User	Configure User Accounts	Configure iRMC S2/S3 Settings	Video Redirection Enabled	Remote Storage Enabled
Select individual Fans (*System Fans* group).						X		
Set *Fan Fail Action / Delay Time.*						X		
Open *Temperature* page	X	X	X	X				
Define action on critical temperature.						X		
Open *Voltages* page.	X	X	X	X				
Open *Power Supply* page.	X	X	X	X				
Configure power supply redundancy						X		
Open *Component Status* page.	X	X	X	X				
Open *System Event Log Content* page.	X	X	X	X				
Clear the system event log (SEL).	X	X	X					
Save event log (SEL).	X	X	X	X				
Define the severity for the display of SEL entries	X	X	X	X				
Open *Internal Event Log Content* page.	X	X						
Clear the internal event log (iEL).	X	X						
Save event log (iEL)	X	X						
Define the severity for the display of SEL entries	X	X						
Open *Event Log Configuration* page.	X	X	X	X				
Edit *System Event Log Configuration* settings.						X		
Edit *Internal Event Log Configuration* settings.						X		
Open/edit *Server Management Info.* page.						X		
Open/edit the *Network Interface* page.						X		

Table 4: Permissions to use special the iRMC S2/S3 web interface

Functions in the iRMC S2/S3 web interface	**Permitted with IPMI privilege level**				**Required iRMC S2/S3-specific permission**			
	OEM	**Administrator**	**Operator**	**User**	**Configure User Accounts**	**Configure iRMC S2/S3 Settings**	**Video Redirection Enabled**	**Remote Storage Enabled**
Open/edit the *Ports and Netw. Services* page.						X		
Open/edit *DNS Configuration* page.						X		
Open/edit *SNMP TRAP Alerting* page.						X		
Open/edit *Serial / Modem Alerting* page.						X		
Open/edit the *Email Alerting* page.						X		
Open/edit the *iRMC S2/S3 User* page.					X			
Open/edit the *Directory Service Config.* page.						X		
Open *CAS Configuration* page					X	X		
Edit *CAS Generic Configuration*						X		
Edit *CAS User Privilege and Permissions*					X			
Open the *BIOS Text Console* page.	X	X	X	X				
Modify the *BIOS Console Redirection Options*.						X		
Start Console Redirection.	X	X	X	X				
Logon in window for power mgmt & text console red.	X	X						
Start the text console (*Enter Console*).	X	X						
Open/edit the *Advanced Video Redirection* page.							X	
Open/edit the *Remote Storage* page.								X
Start *iRMC S2/S3 SSH Access*.	X	X	X	X				
SSH login	X	X	X	X				
Start *iRMC S2/S3 Telnet Access*.	X	X	X	X				
Telnet login	X	X	X	X				

Table 4: Permissions to use special the iRMC S2/S3 web interface

Functions in the iRMC S2/S3 web interface	Permitted with IPMI privilege level				Required iRMC S2/S3-specific permission			
	OEM	Administrator	Operator	User	Configure User Accounts	Configure iRMC S2/S3 Settings	Video Redirection Enabled	Remote Storage Enabled

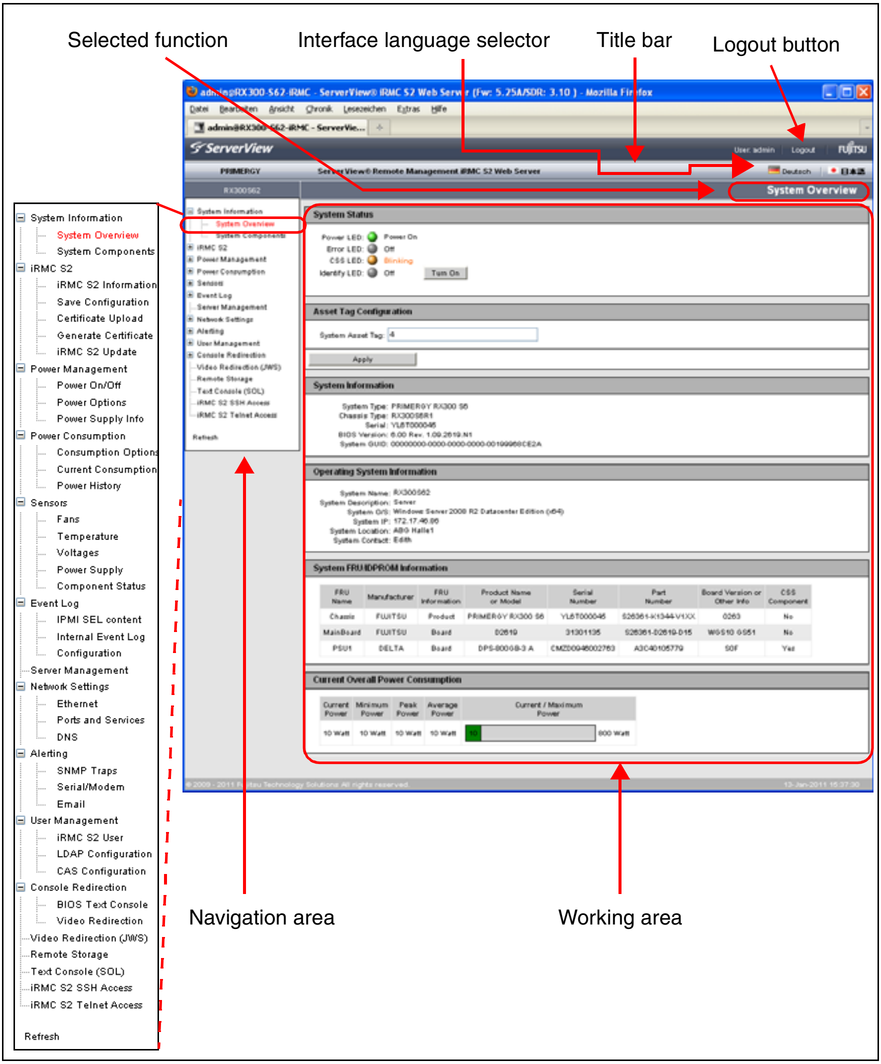
[1] Action is only possible if no agents are running.

[2] Feature is not available on all systems.

Table 4: Permissions to use special the iRMC S2/S3 web interface

7.3 Structure of the user interface

The iRMC S2/S3 web interface is structured as follows:



System Status

Power LED: ● Power On
Error LED: ● Off
CSS LED: ● Blinking
Identify LED: ● Off

Asset Tag Configuration

System Asset Tag: 4

System Information

System Type: PRIMERGY RX300 S6
Chassis Type: RX300S6R1
Serial: YL6T000046
BIOS Version: 6.00 Rev. 1.09.2619.N1
System GUID: 00000000-0000-0000-0000-00199968CE2A

Operating System Information

System Name: RX300S62
System Description: Server
System O/S: Windows Server 2008 R2 Datacenter Edition (x64)
System IP: 172.17.46.86
System Location: ABG Halle1
System Contact: Edith

System FRU IDPROM Information

FRU Name	Manufacturer	FRU Information	Product Name or Model	Serial Number	Part Number	Board Version or Other Info	CSS Component
Chassis	FUJITSU	Product	PRIMERGY RX300 S6	YL6T000046	S26361-K1344-V1XX	0263	No
MainBoard	FUJITSU	Board	D2619	31301135	S26361-D2619-D15	WGS10 GS51	No
PSU1	DELTA	Board	DPS-800GB-3 A	CMZD0946002763	A3C40105779	S0F	Yes

Current Overall Power Consumption

Current Power	Minimum Power	Peak Power	Average Power	Current / Maximum Power	
10 Watt	10 Watt	10 Watt	10 Watt	10	800 Watt

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.   13-Jan-2011 15:37:30

Figure 64: Structure of the iRMC S2/S3 web interface

Choosing the language for the iRMC S2/S3 web interface

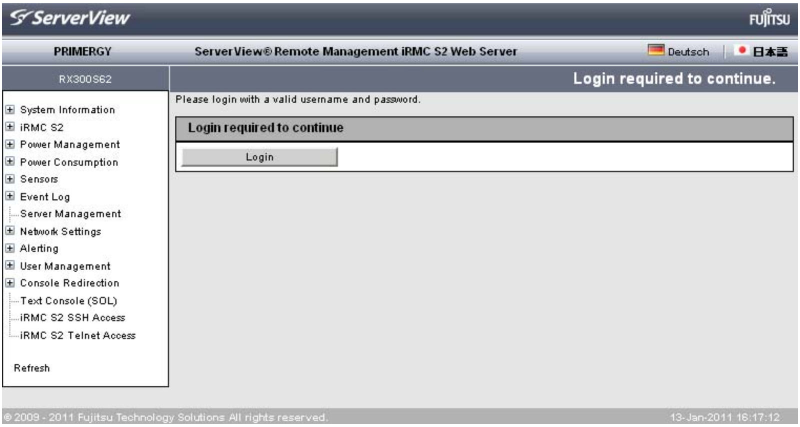
On the right of the black bar above the work area, you will find a flag icon. Click this icon to choose the language (German / English / Japanese) used to display the navigation area, menus and dialog boxes of the iRMC S2/S3 web interface.

Navigation area

The navigation area contains the menu tree structure whose nodes combine the links to the individual iRMC S2/S3 functions arranged on a task basis. When you click one of these links (in figure 64: *System Overview*), the link is enabled and the work area for that function is displayed showing any output, dialog boxes, options, links and buttons.

Below the links to the individual iRMC S2/S3 functions, you will find the links *Logout* and *Refresh*:

- *Logout* allows you to terminate the iRMC S2/S3 session after you have confirmed this in a dialog box. Different login screens appear after the session has been closed depending on whether LDAP access to a directory service has been configured for the iRMC S2/S3 (*LDAP enabled* option, see page 274):
  - If LDAP access to the directory service is not configured for the iRMC S2/S3 (*LDAP enabled* is not activated) and then *Always use SSL login* option (see page 274) is deactivated, the following login screen appears:



Login required to continue.

Please login with a valid username and password.

Login required to continue

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.   13-Jan-2011 16:17:12

Figure 65: Login page (after logging out)

Click *Login* to open the login screen of the iRMC S2/S3 web interface (see figure 62 on page 136). This allows you to log in again if you wish.

- If LDAP access to the directory service is configured for the iRMC S2/S3 (*LDAP enabled* option is activated) or the *Always use SSL login* option (see page 274) is deactivated, the appropriate login screen appears (see figure 63 on page 137).

- Click *Refresh* to refresh the contents of the iRMC S2/S3 web interface.

  ℹ Alternatively, you can configure the interface to automatically update the contents periodically (see "Enable Auto Refresh" on page 246).

7.4 System Information - Information on the server

The *System Information* entry contains the links to the following pages:

– "System Overview - General information on the server" on page 147

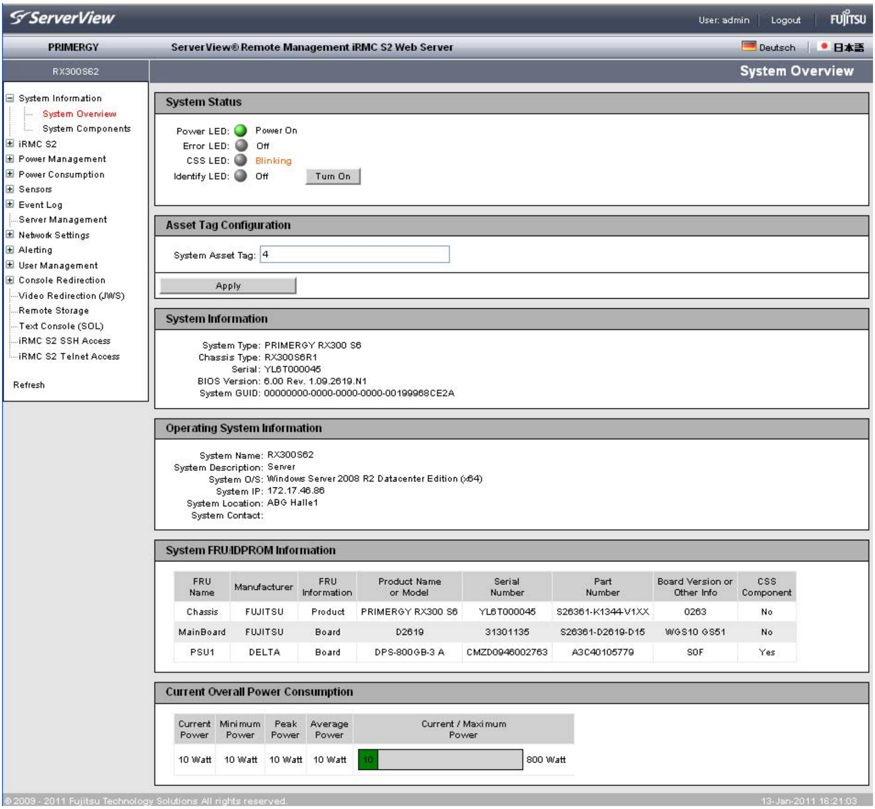
– "System Component Information - Information on the server components" on page 152

7.4.1 System Overview - General information on the server

The *System Overview* page provides information on

- the system status,
- system (general information)
- the operating system of the managed server,
- system FRUs (Field Replaceable Units) / IDPROM.
- current overall power consumption of the managed server

In addition, the *System Overview* page allows you to enter a customer-specific asset tag for the managed server.



System Status

Power LED: ● Power On
Error LED: ● Off
CSS LED: ● Blinking
Identify LED: ● Off

Asset Tag Configuration

System Asset Tag: 4

System Information

System Type: PRIMERGY RX300 S6
Chassis Type: RX300S6R1
Serial: YL6T000045
BIOS Version: 6.00 Rev. 1.09.2619.N1
System GUID: 00000000-0000-0000-0000-00199968CE2A

Operating System Information

System Name: RX300S62
System Description: Server
System O/S: Windows Server 2008 R2 Datacenter Edition (x64)
System IP: 172.17.46.86
System Location: ABG Halle1
System Contact:

System FRU/IDPROM Information

FRU Name	Manufacturer	FRU Information	Product Name or Model	Serial Number	Part Number	Board Version or Other Info	CSS Component
Chassis	FUJITSU	Product	PRIMERGY RX300 S6	YL6T000045	S26361-K1344-V1XX	0263	No
MainBoard	FUJITSU	Board	D2619	31301135	S26361-D2619-D15	WGS10 GS51	No
PSU1	DELTA	Board	DPS-800GB-3 A	CMZD0946002763	A3C40105779	S0F	Yes

Current Overall Power Consumption

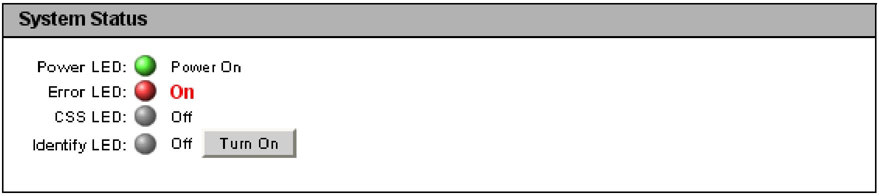
Current Power	Minimum Power	Peak Power	Average Power	Current / Maximum Power
10 Watt	10 Watt	10 Watt	10 Watt	10 800 Watt

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.
13-Jan-2011 16:21:03

Figure 66: System Overview page

System Status

The status of the global error LED, the CSS LED and the identification LED are shown under *System Status*. You can also switch the PRIMERGY identification LED on and off.



System Status

Power LED: ● Power On

Error LED: ● On

CSS LED: ● Off

Identify LED: ● Off

Figure 67: System Overview page - System Status

Power LED

Power status of the server.
The following statuses are possible:

- On: “Power ON” (green)
- On: “Standby mode (green) with text “Suspend to RAM (Standby)”.
- Off: “Power OFF” (orange)

Error LED

Informs about the server‘s Global Error LED:

Status Info (iRMC S2/S3)	Global Error LED on the Server	Status of the servers
off	does not light up.	No critical event.
on	lights red.	Prefailure event for a non CSS component.
blinking	flashes red.	Critical event.

CSS LED

Informs about the server’s CSS (Customer Self Service) LED:

Status Info (iRMC S2/S3)	CSS LED on the Server	Status of the server
off	does not light up.	The server is operational.
on	lights orange.	Prefailure event for a CSS component.
blinking	flashes orange.	Defective CSS component.

Identify LED

Server identifier.
The following statuses are possible:

- On (blue)
- Off (grey)

Turn On/Turn Off

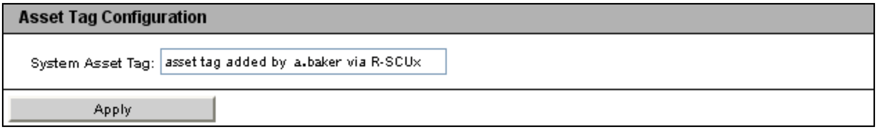
Click *Turn On / Turn Off* to toggle the PRIMERGY identification LED on and off.

Asset Tag Configuration

Under *Asset Tag Configuration*, you can enter a customer-specific asset tag for the managed server.

The customer-specific asset tag allows you to assign the server an inventory number or other identifier of your choice.

With Windows-based systems, this customer-specific asset tag is provided automatically by the WMI (Windows Management Instrumentation). It can then be evaluated by in-house tools or used for integration in enterprise management systems (such as CA Unicenter).



Asset Tag Configuration

System Asset Tag: asset tag added by a.baker via R-SCUx

Figure 68: The System Overview - System Status page

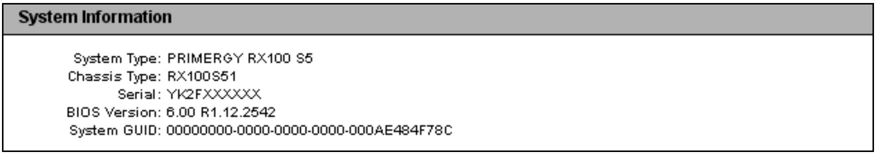
System Asset Tag

You can enter the asset tag here.

► Click *Apply* to accept the asset tag.

System Information

System Information lists information on the managed server.



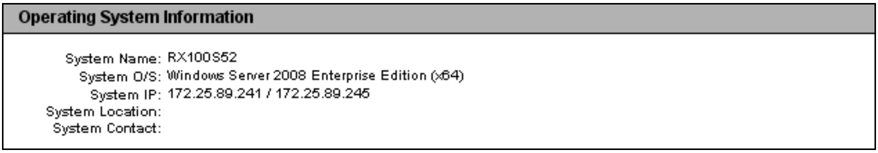
System Information

```
   System Type: PRIMERGY RX100 S5
  Chassis Type: RX100S51
        Serial: YK2FXXXXXX
  BIOS Version: 6.00 R1.12.2542
   System GUID: 00000000-0000-0000-0000-000AE484F78C
```

Figure 69: System Overview page - System Information

Operating System Information

Operating System Information lists information on the operating system of the managed server.



Operating System Information

```
    System Name: RX100S52
     System O/S: Windows Server 2008 Enterprise Edition (x64)
      System IP: 172.25.89.241 / 172.25.89.245
System Location:
 System Contact:
```

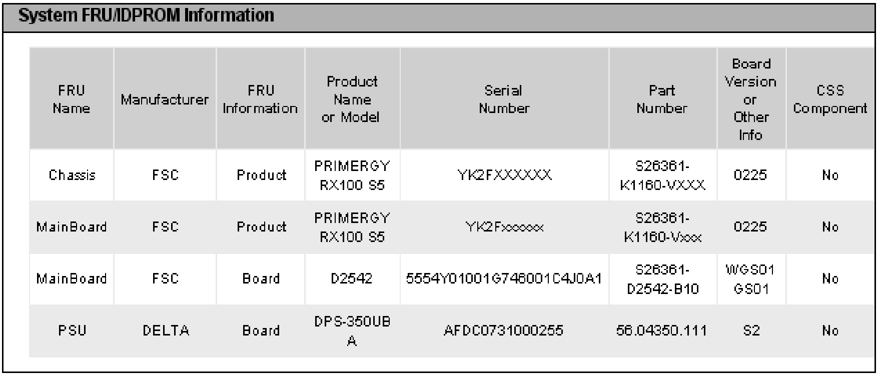
Figure 70: System Overview page - Operating System Information

i If no ServerView agents are running, you can edit the *System Location* and *System contact* fields, otherwise these fields are not editable.

After the ServerView agents have been started, your initial values will be overwritten by the values automatically detected by the agents.

System FRU / IDPROM Information

Information on the FRUs (**F**ield **R**eplaceable **U**nits) is listed under *System FRU/IDPROM Information*. FRUs are system components that can be released and removed from the system. The *CSS Component* column indicates for each of the components whether the CSS (**C**ustomer **S**elf **S**ervice) functionality is supported.



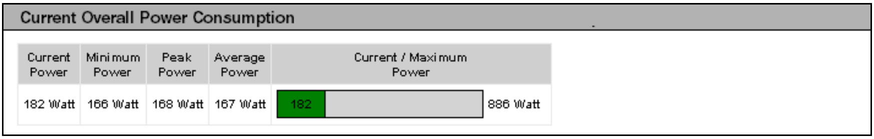
System FRU/IDPROM Information

FRU Name	Manufacturer	FRU Information	Product Name or Model	Serial Number	Part Number	Board Version or Other Info	CSS Component
Chassis	FSC	Product	PRIMERGY RX100 S5	YK2FXXXXXX	S26361-K1160-VXXX	0225	No
MainBoard	FSC	Product	PRIMERGY RX100 S5	YK2Fxxxxxx	S26361-K1160-Vxxx	0225	No
MainBoard	FSC	Board	D2542	5554Y01001G746001C4J0A1	S26361-D2542-B10	WGS01 GS01	No
PSU	DELTA	Board	DPS-350UB A	AFDC0731000255	56.04350.111	S2	No

Figure 71: System Overview page - System FRU / IDPROM Information

Current Overall Power Consumption

This option is not supported for all PRIMERGY servers.



Current Overall Power Consumption

Current Power	Minimum Power	Peak Power	Average Power	Current / Maximum Power
182 Watt	166 Watt	168 Watt	167 Watt	182 886 Watt

Figure 72: System Overview page - Current Overall Power Consumption

Under *Current Overall Power Consumption* you can see all the measurements current, minimum, maximum and average power consumption for the server in the current interval.

A graphical display also shows the current power consumption of the server compared with the maximum possible power consumption.

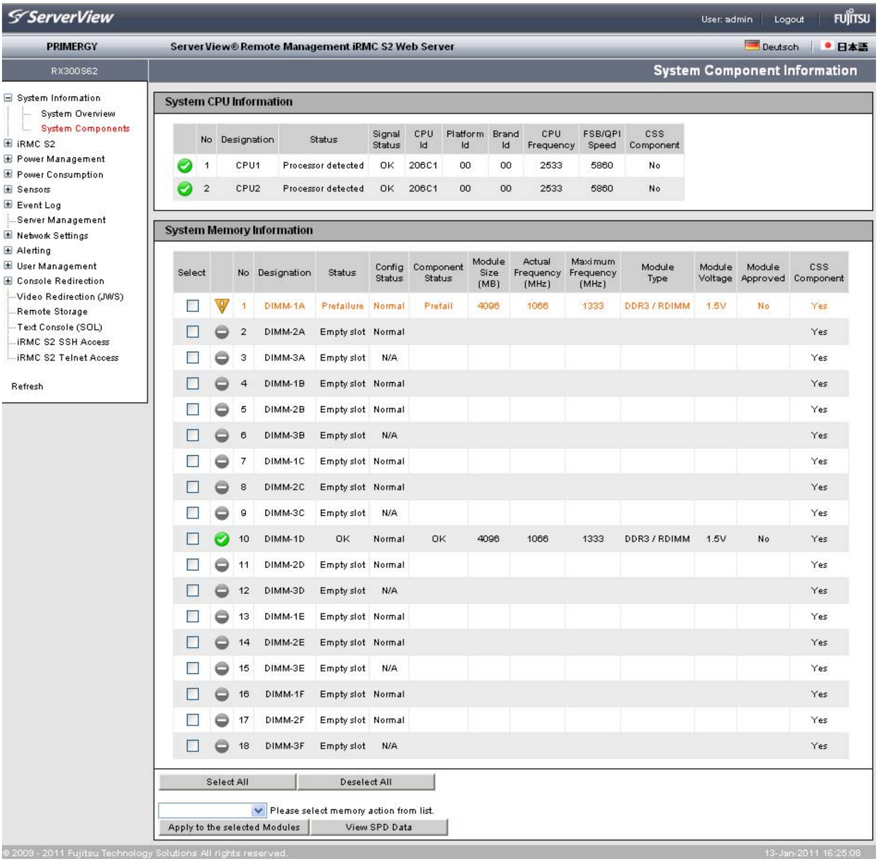
7.4.2 System Component Information - Information on the server components

The *System Component Information* page provides information on the CPU and the main memory modules. The *CSS Component* column indicates for each of the components whether the CSS (**C**ustomer **S**elf **S**ervice) functionality is supported.

The following status icons indicate the possible statuses of the system components:

✓	OK: Component status is okay.
⊖	Component slot is empty.
⚠	Warning: The status of the component has deteriorated.
✖	Fault: The component has a fault.

Table 5: Status of the system component



ServerView® Remote Management iRMC S2 Web Server

System Component Information

- ⊟ System Information
  - System Overview
  - System Components
- ⊞ iRMC S2
- ⊞ Power Management
- ⊞ Power Consumption
- ⊞ Sensors
- ⊞ Event Log
- Server Management
- ⊞ Network Settings
- ⊞ Alerting
- ⊞ User Management
- ⊞ Console Redirection
- Video Redirection (JWS)
- Remote Storage
- Text Console (SOL)
- iRMC S2 SSH Access
- iRMC S2 Telnet Access

Refresh

System CPU Information

	No	Designation	Status	Signal Status	CPU Id	Platform Id	Brand Id	CPU Frequency	FSB/QPI Speed	CSS Component
✓	1	CPU1	Processor detected	OK	206C1	00	00	2533	5860	No
✓	2	CPU2	Processor detected	OK	206C1	00	00	2533	5860	No

System Memory Information

Select		No	Designation	Status	Config Status	Component Status	Module Size (MB)	Actual Frequency (MHz)	Maximum Frequency (MHz)	Module Type	Module Voltage	Module Approved	CSS Component
□	⚠	1	DIMM-1A	Prefailure	Normal	Prefail	4096	1066	1333	DDR3 / RDIMM	1.5V	No	Yes
□	⊖	2	DIMM-2A	Empty slot	Normal								Yes
□	⊖	3	DIMM-3A	Empty slot	N/A								Yes
□	⊖	4	DIMM-1B	Empty slot	Normal								Yes
□	⊖	5	DIMM-2B	Empty slot	Normal								Yes
□	⊖	6	DIMM-3B	Empty slot	N/A								Yes
□	⊖	7	DIMM-1C	Empty slot	Normal								Yes
□	⊖	8	DIMM-2C	Empty slot	Normal								Yes
□	⊖	9	DIMM-3C	Empty slot	N/A								Yes
□	✓	10	DIMM-1D	OK	Normal	OK	4096	1066	1333	DDR3 / RDIMM	1.5V	No	Yes
□	⊖	11	DIMM-2D	Empty slot	Normal								Yes
□	⊖	12	DIMM-3D	Empty slot	N/A								Yes
□	⊖	13	DIMM-1E	Empty slot	Normal								Yes
□	⊖	14	DIMM-2E	Empty slot	Normal								Yes
□	⊖	15	DIMM-3E	Empty slot	N/A								Yes
□	⊖	16	DIMM-1F	Empty slot	Normal								Yes
□	⊖	17	DIMM-2F	Empty slot	Normal								Yes
□	⊖	18	DIMM-3F	Empty slot	N/A								Yes

Please select memory action from list.

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.

13-Jan-2011 16:25:08

Figure 73: System Component Information page

On PRIMERGY servers with support for TPM (Trusted Platform Module), this page indicates whether TPM is enabled or disabled.

System CPU Information

This group provides information on the status, IDs, CSS capability and performance of the CPU(s) in the managed PRIMERGY server.

System Memory Information

This group provides information on the status, IDs, CSS capability and performance of the main memory modules in the managed PRIMERGY server.

Select

Here you can select individual memory modules to which the action you select under *Please select memory action from* list is to be applied.

Select all

Selects all memory modules.

Deselect all

Cancels your selection.

Please select memory action from list

This list allows you to select an action to be applied to the selected memory modules.

Apply to the selected modules

Applies the selected action to the selected memory modules.

View SPD Data / No SPD Data

Clicking the toggle button *View SPD Data / No SPD Data* shows or hides vendor-specific details (**S**erial **P**resence **D**etect (SPD) data) for the individual memory components.

The SPD data for a memory component is stored in an EEPROM integrated in the component and serves to allow the BIOS to automatically detect this memory component (RAM, DIMM).

7.5 BIOS - Backing up/restore BIOS settings, flashing BIOS

The *BIOS* entry contains the links to the following pages:

– "Backup/Restoration - Saving/Restoring BIOS single parameter settings to/from a file" on page 155

– "BIOS - Updating BIOS via "upload from file" or via TFTP" on page 159

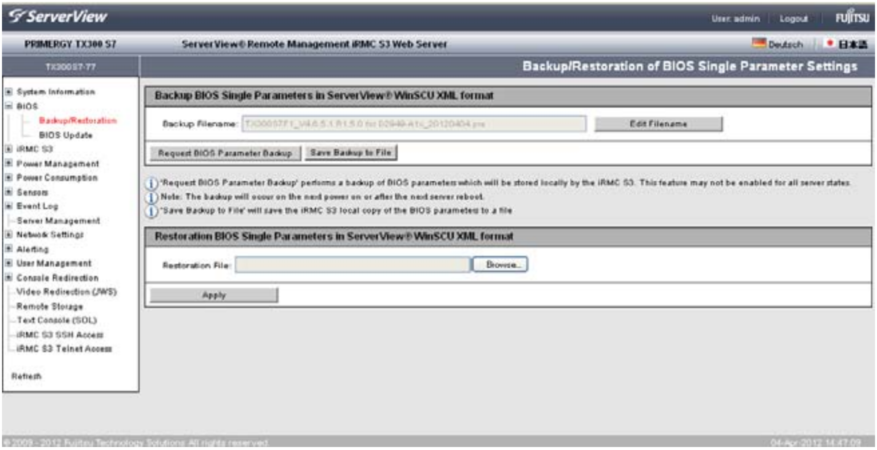
i These pages are only displayed if the BIOS of the managed server supports the corresponding feature requirements.

7.5.1 Backup/Restoration - Saving/Restoring BIOS single parameter settings to/from a file

The *Backup/Restoration of BIOS Single Parameter Settings* page provides you with the following options:

– Back up single BIOS parameters in ServerView® WinSCU XML format and save the backup to a file.

– Restore single BIOS parameter settings in ServerView® WinSCU XML format from a file.



Backup Filename: TX300S7F1_V4.6.5.1 R1.5.0 for D2949-A1x_20120404.pre

'Request BIOS Parameter Backup' performs a backup of BIOS parameters which will be stored locally by the iRMC S3. This feature may not be enabled for all server states.

Note: The backup will occur on the next power on or after the next server reboot.

'Save Backup to File' will save the iRMC S3 local copy of the BIOS parameters to a file

Restoration File:

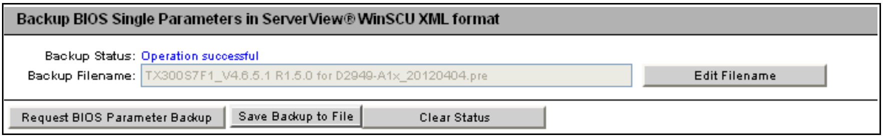
© 2009 - 2012 Fujitsu Technology Solutions All rights reserved.

04-Apr-2012 14:47:09

Figure 74: Backup/Restoration of BIOS Single Parameter Settings page

7.5.1.1 Backing up single BIOS parameters in ServerView® WinSCU XML format

The *Backup BIOS Single Parameters in ServerView® WinSCU XML format* group allows you to back up single BIOS parameter settings in ServerView® WinSCU XML format and to save the backup to a file.



Backup BIOS Single Parameters in ServerView® WinSCU XML format

Backup Status: Operation successful

Backup Filename: TX300S7F1_V4.6.5.1 R1.5.0 for D2949-A1x_20120404.pre

Figure 75: Backup BIOS Single Parameters in ServerView® WinSCU XML format

Backup Status

Displays the status of the current backup process. Successful completion is indicated by "Operation Successful". The *Backup Status* is only displayed if a backup is currently in process or has completed.

You can clear the status display by clicking the *Clear Status* button, which is only available if a status is currently displayed.

Clear Status

Clears the status information indicated under *Backup Status*. This button is only available if a status is currently displayed under *Backup Status*.

Backup Filename

This input field is disabled ("grayed out") by default. Initially, it displays the file name that is dynamically generated by the iRMC S2/S3.

Edit Filename

Enables the *Backup Filename* field, thus allowing you to enter a file name (*.pre*) of your choice.

Save Filename

Saves the edited file name, which, starting from now, will be the name displayed by default in the *Backup Filename* field.

Request BIOS Parameter Backup

Initiates a backup of single BIOS parameter settings in ServerView® WinSCU XML format. The backup (with the name specified in the *Backup Filename* field) is stored locally on the iRMC S2/S3.

Once the backup process has started, the current process status is displayed under *Backup Status*.

Notes on the backup process:

– During the backup process, all buttons and input fields are disabled.

– If powered off, the managed server will be automatically powered on.

– If the server is powered on, a reboot is required. Otherwise, the backup process will remain in state "Boot Pending".

– The managed server is powered off after the backup has completed.

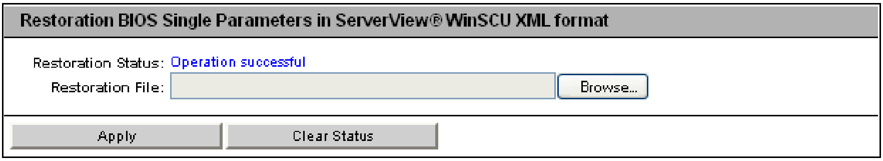
Save Backup to File

Opens a browser dialog allowing you to save the iRMC S2/S3-local copy of the BIOS backup data to a file (*<name -of-your-choice>.pre*).

This button is only displayed when a backup of single BIOS parameters in ServerView® WinSCU XML format is available in the local store of the iRMC S2/S3.

7.5.1.2 Restoring single BIOS parameters in ServerView® WinSCU XML format

The *Restoration BIOS Single Parameters in ServerView® WinSCU XML format* group allows you to restore single BIOS parameter settings from a restoration file in ServerView® WinSCU XML format.


Restoration BIOS Single Parameters in ServerView® WinSCU XML format

Restoration Status: Operation successful

Restoration File:

Figure 76: Restoration BIOS Single Parameters in ServerView® WinSCU XML format

Restoration Status

Displays the status of the current restoration process. Successful completion is indicated by "Operation successful". The *Restoration Status* is only displayed if a restoration is currently in process or has completed.

You can clear the status display by clicking the *Clear Status* button, which is only available if a status is currently displayed.

Clear Status

Clears the status information indicated under *Restoration Status*. This button is only displayed if a status is currently indicated under *Restoration Status*.

Restoration File

Clicking the input field or clicking *Browse...* opens a browser dialog allowing you to navigate to a file (*.pre*) containing a backup of single BIOS parameters in the ServerView® WinSCU XML format.

Apply

Initiates the restoration of single BIOS parameter settings based on the file specified in the *Restoration File* field.

Once the restoration process has started, the current process status is indicated under *Restoration Status*.

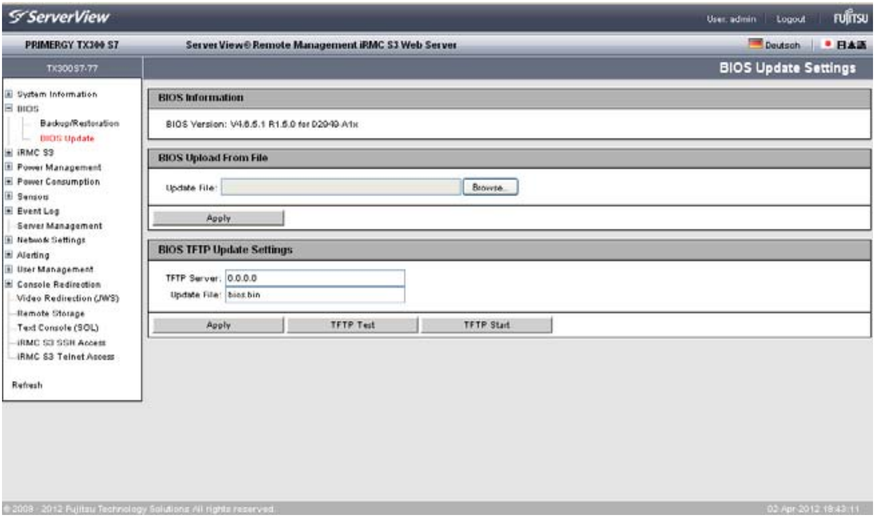
Notes on the restoration process:

- During the restoration process, all buttons and input fields are disabled.
- If powered off, the managed server will automatically be powered on.
- If the managed server is powered on, the server is to be rebooted. Otherwise the restoration process will remain in state "Boot Pending".
- The managed server is powered off after the restoration has completed.

7.5.2 BIOS - Updating BIOS via "upload from file" or via TFTP

The *BIOS Update Settings* page provides information on the current BIOS version on the managed server and allows you to update the BIOS via "upload from file" or via TFTP.

> i You will find the appropriate BIOS image for your PRIMERGY server on ServerView Suite DVD 1 or you can download it under *http://support.ts.fujitsu.com/com/support/downloads.html*.



BIOS Version: V4.6.5.1 R1.5.0 for D2949-A1x

Update File:

TFTP Server: 0.0.0.0

Update File: bios.bin

© 2009 - 2012 Fujitsu Technology Solutions All rights reserved.   02 Apr 2012 18:43:11

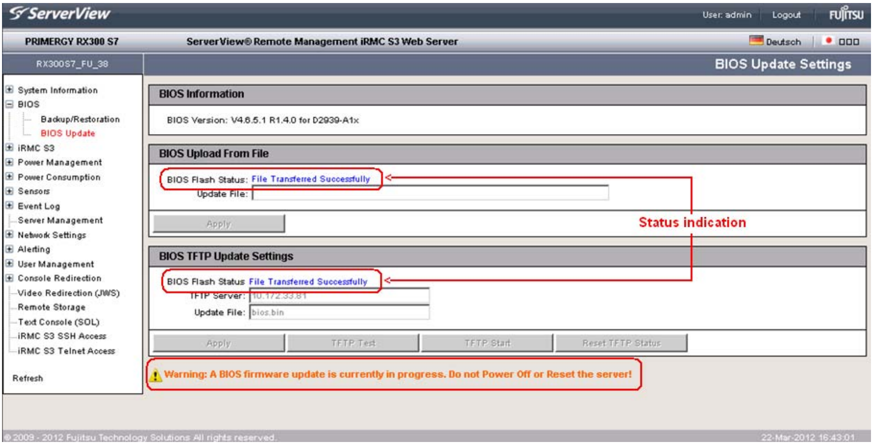
Figure 77: BIOS Update Settings page

Updating (flashing) the BIOS - course of events and important notes

The following overview applies for both updating the BIOS via "upload from file" and updating the BIOS via TFTP.

> **i** Details on how to initiate the steps described in this overview are described below in this section.

> **i** During the complete update process, the current update status is indicated in the *BIOS Update Settings* page.



BIOS Update Settings

BIOS Information

BIOS Version: V4.6.5.1 R1.4.0 for D2939-A1x

BIOS Upload From File

BIOS Flash Status: File Transferred Successfully
Update File:

BIOS TFTP Update Settings

BIOS Flash Status File Transferred Successfully
TFTP Server: 10.172.33.81
Update File: bios.bin

Warning: A BIOS firmware update is currently in progress. Do not Power Off or Reset the server!

Figure 78: Updating BIOS - (TFTP) download successfully finished

Updating the BIOS comprises the following steps:

1. In the first step, you download the update file.

   > **i** The update file must be a *UPC* file.

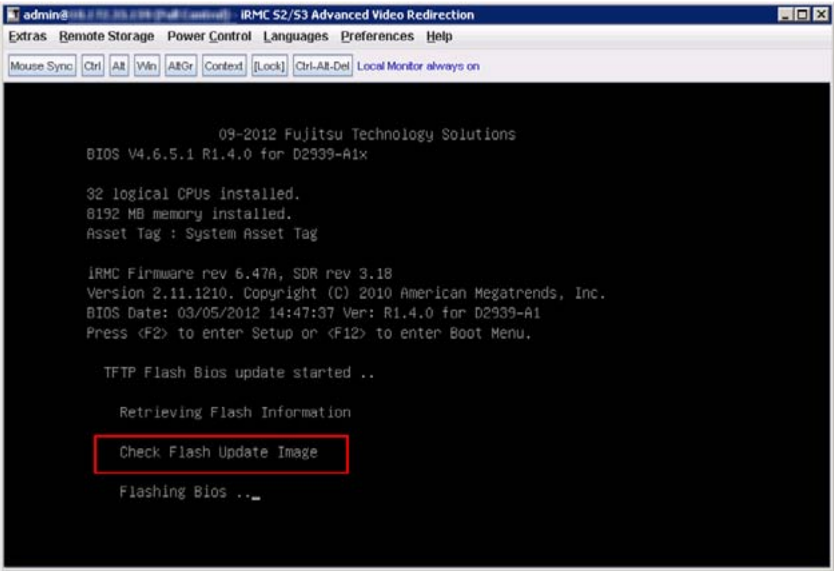
   After the update file has been downloaded, the following occurs:

   – If the server is powered off, the server will be automatically powered on to initiate the flash process.

   – If the server is already powered on, you must restart the server to initiate the flash process.

   > **CAUTION!**
   >
   > If a BIOS update is currently in progress, do **not** power-off or restart the server.

2. Subsequently, flash data is transferred to memory. The status display will indicate when the transfer has successfully completed.
3. Before the actual flashing process is started, the flash/update image is checked.



```
                 09-2012 Fujitsu Technology Solutions
BIOS V4.6.5.1 R1.4.0 for D2939-A1x

32 logical CPUs installed.
8192 MB memory installed.
Asset Tag : System Asset Tag

iRMC Firmware rev 6.47A, SDR rev 3.18
Version 2.11.1210. Copyright (C) 2010 American Megatrends, Inc.
BIOS Date: 03/05/2012 14:47:37 Ver: R1.4.0 for D2939-A1
Press <F2> to enter Setup or <F12> to enter Boot Menu.

  TFTP Flash Bios update started ..

    Retrieving Flash Information

    Check Flash Update Image

    Flashing Bios .._
```

Figure 79: Updating BIOS - checking update/flash image

4. Once the update/flash image is successfully verified, the actual flashing process is started. The status indication shows the percentage completion of the flash process.
5. After the BIOS update has successfully completed, the server is powered off. The following entry is written to the system event log (SEL):

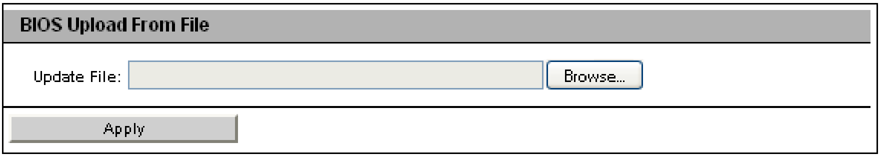
   ```
   BIOS TFTP or HTTP/HTTPS flash OK
   ```

BIOS Information

This group provides information on the current BIOS version on the managed server.

BIOS Upload from File

The *BIOS Upload from File* group allows you to perform an online update of the BIOS on the managed server. To do this, you must provide the current BIOS image in a file.



BIOS Upload From File

Update File: [ ] Browse...

Apply

Figure 80: BIOS Update Settings page - BIOS Update from File

Update file

File in which the BIOS image is stored.

> A *UPC*-format file is required for performing the *BIOS Upload from File* function.

Browse...

Opens a file browser that allows you to navigate to the update file.

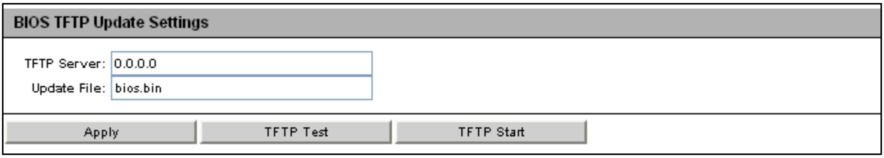
► Click *Apply* to activate your settings and to start flashing the BIOS.

CAUTION!

If a BIOS update is currently in progress, do **not** power-off or restart the server.

BIOS TFTP Update Settings

The *BIOS TFTP Update Settings* group allows you to perform an online update of the BIOS on the managed server. To do this, you must provide the current BIOS image in a file on a TFTP server. The BIOS is flashed when TFTP is started.



BIOS TFTP Update Settings

TFTP Server: 0.0.0.0

Update File: bios.bin

Figure 81: BIOS Update Settings page - BIOS TFTP Update Settings

TFTP Server

IP address or DNS name of the TFTP server on which the file with the BIOS image is stored.

Update file

File in which the BIOS image is stored.

i A *UPC*-format file is required for performing the *BIOS TFTP Update Settings* function.

► Click *Apply* to activate your settings.

► Click *TFTP Test* to test the connection to the TFTP server.

► Click *TFTP Start* to download the file containing the BIOS image from the TFTP server and to start flashing the BIOS.

CAUTION!

If a BIOS update is currently in progress, do **not** power-off or restart the server.

7.6 iRMC S2/S3 - Information, firmware and certificates

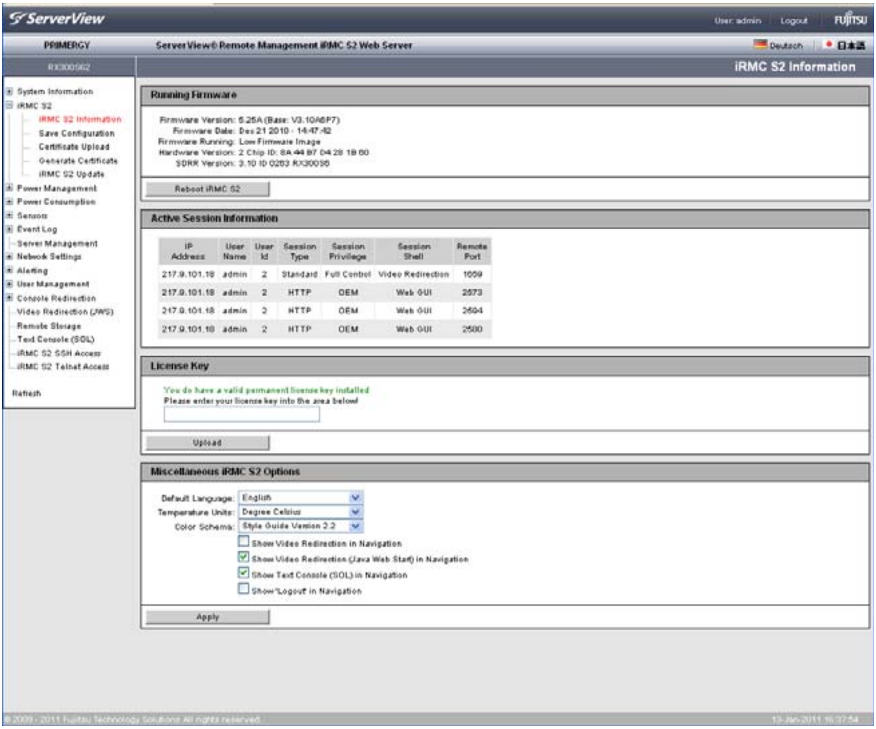
The *iRMC S2/S3* entry contains the links to the following pages:

- "iRMC S2/S3 Information - Information on the iRMC S2/S3" on page 165
- "Save iRMC S2/S3 Firmware Settings - Save firmware settings" on page 169
- "Certificate Upload - Load the DSA/RSA certificate and private DSA/RSA key" on page 172.
- "Generate a self-signed Certificate - Generate self-signed RSA certificate" on page 179
- "iRMC S2/S3 Firmware Update" on page 181

7.6.1 iRMC S2/S3 Information - Information on the iRMC S2/S3

The *iRMC S2/S3 Information* page provides you with the following options:

- View information on the firmware and the SDRR version of the iRMC S2/S3, set the firmware selector and load a firmware image and restart the iRMC S2/S3.
- View information on the active iRMC S2/S3 sessions.
- Load license key onto the iRMC S2/S3.
- Make settings for the layout of the iRMC S2/S3 web interface.



Running Firmware

Firmware Version: 5.25A (Base: V3.10A6P7)
Firmware Date: Dec 21 2010 - 14:47:42
Firmware Running: Low Firmware Image
Hardware Version: 2 Chip ID: 8A 44 B7 D4 28 18 60
SDRR Version: 3.10 ID 0283 RX300S6

Active Session Information

IP Address	User Name	User Id	Session Type	Session Privilege	Session Shell	Remote Port
217.9.101.18	admin	2	Standard	Full Control	Video Redirection	1659
217.9.101.18	admin	2	HTTP	OEM	Web GUI	2573
217.9.101.18	admin	2	HTTP	OEM	Web GUI	2604
217.9.101.18	admin	2	HTTP	OEM	Web GUI	2500

License Key

You do have a valid permanent license key installed
Please enter your license key into the area below!

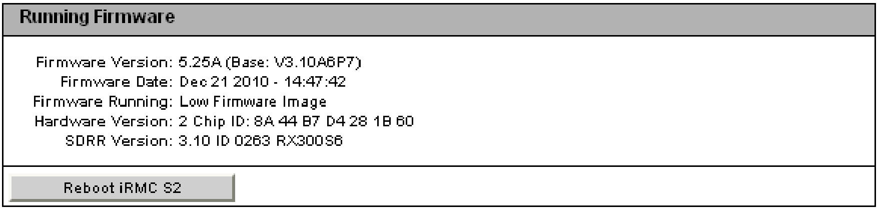
Miscellaneous iRMC S2 Options

Default Language: English
Temperature Units: Degree Celsius
Color Schema: Style Guide Version 2.2
☐ Show Video Redirection in Navigation
☑ Show Video Redirection (Java Web Start) in Navigation
☑ Show Text Console (SOL) in Navigation
☐ Show "Logout" in Navigation

Figure 82: iRMC S2/S3 Information page

Running Firmware

Under *Running Firmware*, you can view information on the firmware and the SDRR version of the iRMC S2/S3 and restart the iRMC S2/S3.



Running Firmware

Firmware Version: 5.25A (Base: V3.10A6P7)
Firmware Date: Dec 21 2010 - 14:47:42
Firmware Running: Low Firmware Image
Hardware Version: 2 Chip ID: 8A 44 B7 D4 28 1B 60
SDRR Version: 3.10 ID 0263 RX300S6

Figure 83: iRMC S2/S3 Information page - Firmware Information and iRMC S2/S3 reboot

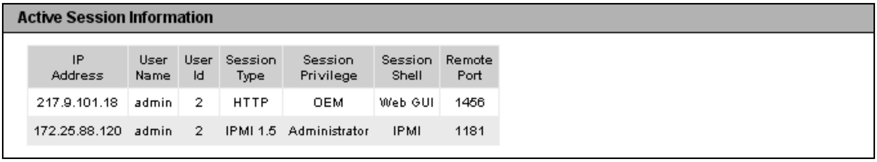
Reboot iRMC S2/S3

Reboots the iRMC S2/S3.

The *Reboot iRMC S2/S3* button is disabled during the BIOS POST phase of the managed server.

Active Session Information

The *Active Session Information* group shows all the currently active iRMC S2/S3 sessions.



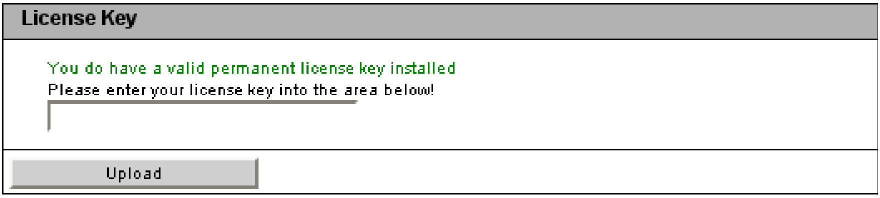
Active Session Information

IP Address	User Name	User Id	Session Type	Session Privilege	Session Shell	Remote Port
217.9.101.18	admin	2	HTTP	OEM	Web GUI	1456
172.25.88.120	admin	2	IPMI 1.5	Administrator	IPMI	1181

Figure 84: iRMC S2/S3 Information page - Active Session Information

License Key

The *License Key* group allows you to load a license key onto the iRMC S2/S3.



License Key

You do have a valid permanent license key installed
Please enter your license key into the area below!

Figure 85: iRMC S2/S3 Information page - License Key

You require a valid license key to be able to use the iRMC S2/S3 functions *Advanced Video Redirection* (see page 302) and *Remote Storage* (see page 312).

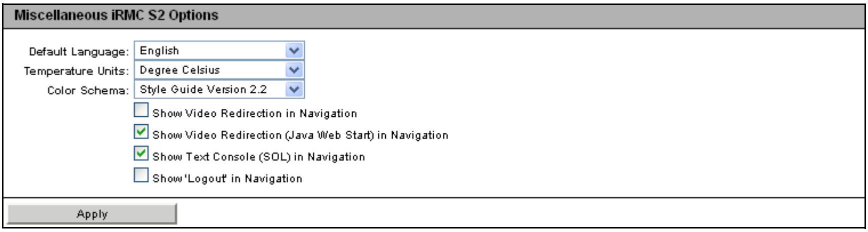
You can purchase the license key.

Upload

When you click this button, the license key specified in the input field is loaded onto the iRMC S2/S3.

Miscellaneous iRMC S2/S3 Options

The *Miscellaneous iRMC S2/S3 Options* group allows you to make settings for the layout of the iRMC S2/S3 web interface.



Miscellaneous iRMC S2 Options

Default Language: English

Temperature Units: Degree Celsius

Color Schema: Style Guide Version 2.2

□ Show Video Redirection in Navigation

☑ Show Video Redirection (Java Web Start) in Navigation

☑ Show Text Console (SOL) in Navigation

□ Show 'Logout' in Navigation

Figure 86: iRMC Information page - Miscellaneous Options

Default Language

Specifies the language (German / English / Japanese) that is set as default the next time the iRMC S2/S3 web interface is called.

Temperature Units

Specifies the unit used for displaying temperature values at the iRMC S2/S3 web interface (degrees Celsius / degrees Fahrenheit). This setting applies for the current session and is preset the next time the iRMC S2/S3 web interface is called.

Colour Schema

Specifies the color scheme for displaying the iRMC S2/S3 web interface. This setting applies for the current session and is preset the next time the iRMC S2/S3 web interface is called.

Show Video Redirection in Navigation

Adds the *Video Redirction* link to the navigation area. This link allows you to directly start video redirection (see "Video Redirection - Starting AVR" on page 308).

Show Video Redirection (Java Web Start) in Navigation

Adds the *Video Redirction (JWS)* link to the navigation area. This allows you to directly start video redirection (Java Web Start) (see "Video Redirection - Starting AVR" on page 308).

Show the Text Console (SOL) in Navigation

Adds the *Text Console (SOL)* link to the navigation area. This allows you to directly start text console redirection (see section "Text Console Redirection (via Serial over LAN) - Start text console redirection" on page 295).

Show the 'Logout' in Navigation

This option is only available if the iRMC S2/S3 information page is displayed in the *StyleguideVersion 2.2* color scheme.

Adds the *Logout* link to the navigation area. This allows you to logout via the navigation area.

7.6.2 Save iRMC S2/S3 Firmware Settings - Save firmware settings

The *Save iRMC S2/S3 Firmware Settings* page allows you to save the current firmware settings and a number of other settings for the iRMC S2/S3 in a file. Additionally, you can load the firmware settings onto the iRMC S2/S3 again.

– The firmware settings selected under *Save iRMC S2/S3 Firmware settings in ServerView® WinSCU XML format* are saved in a file with the name *iRMC_S2_settings.pre* or *iRMC_ S3_settings.pre*, respectively. In the Server Configuration Manager (WinSCU), you can use the *Import...* button to load the firmware settings onto the iRMC S2/S3 again.

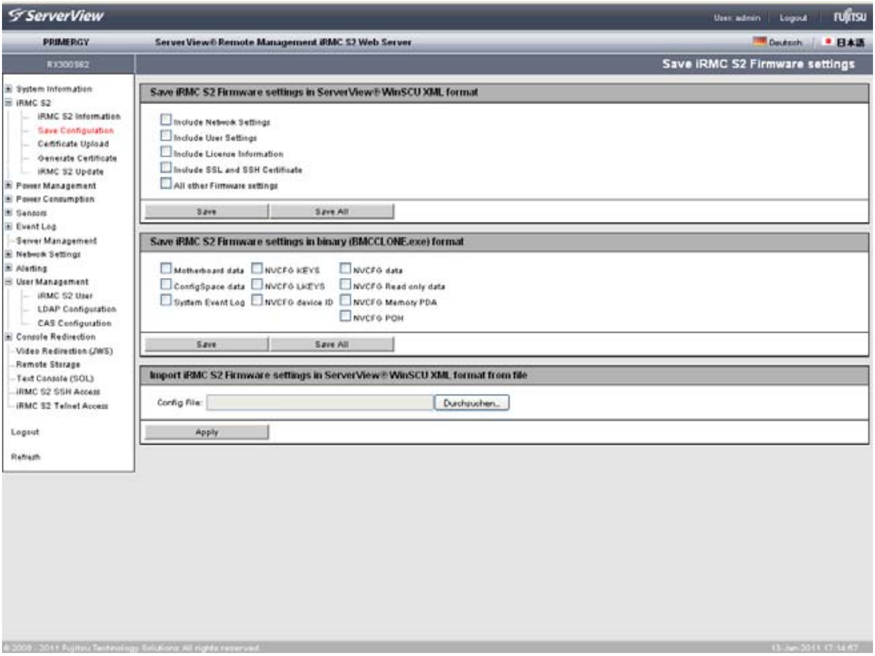
– The firmware settings selected under *Save iRMC S2/S3 Firmware settings in binary (BMCCLONE.exe) format* are saved in a file with the name *iRMC_S2_settings.bin* or iRMC_ S3_settings.bin, respectively. You can use the *Import iRMC S2/S3 Firmware settings in ServerView® WinSCU XML format from file* group to load the firmware settings onto the iRMC S2/S3 again.

CAUTION!

Always save the setting using *Save iRMC S2/S3 Firmware settings in ServerView® WinSCU XML format*.

Save iRMC S2/S3 Firmware settings in binary (BMCCLONE.exe) format should only be used if the system module of the managed server is being replaced.

If you want to save the user settings *(Include User Settings*), you require *Configure User Accounts* permission. In all other cases, *Configure iRMC S2/S3 settings* permission is sufficient.



Save iRMC S2 Firmware settings

Save iRMC S2 Firmware settings in ServerView® WinSCU XML format

☐ Include Network Settings
☐ Include User Settings
☐ Include License Information
☐ Include SSL and SSH Certificate
☐ All other Firmware settings

Save iRMC S2 Firmware settings in binary (BMCCLONE.exe) format

☐ Motherboard data	☐ NVCFG KEYS	☐ NVCFG data
☐ ConfigSpace data	☐ NVCFG LKEYS	☐ NVCFG Read only data
☐ System Event Log	☐ NVCFG device ID	☐ NVCFG Memory PDA
		☐ NVCFG POH

Import iRMC S2 Firmware settings in ServerView® WinSCU XML format from file

Config File:

Figure 87: Save iRMC S2/S3 Firmware Settings page

Save iRMC S2/S3 firmware settings ...

The data is exported from the iRMC S2/S3 in logical sections, each corresponding to a selected option.

The option *All other Firmware settings* causes the firmware to export all current ConfigSpace values that have not already been exported together with another section. New implemented values are automatically exported with newer firmware versions.

Save

Click *Save* to save the selected settings.

Save All

Click *Save All* to save all the settings.

Import iRMC S2/S3 Firmware settings in ServerView® WinSCU XML format from file

Config File

Configuration file (default: *iRMC_S2_settings.bin* / *iRMC_S3_settings.bin*) in the ServerView® WinSCU XML format from which you want to load the firmware settings onto the iRMC S2/S3.

Browse

Opens a file browser that allows you to navigate to the configuration file.

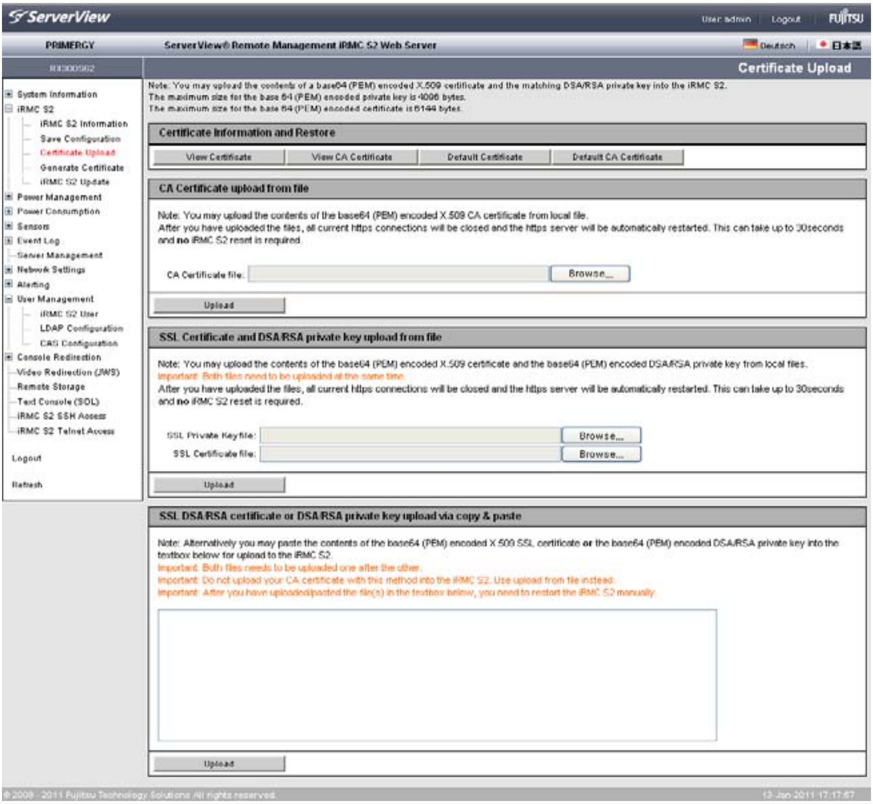
7.6.3 Certificate Upload - Load the DSA/RSA certificate and private DSA/RSA key

The *Certificate Upload* page allows you to load a signed X.509 DSA/RSA certificate (SSL) from a Certificate Authority (CA) and/or your private DSA/RSA key (SSH) onto the iRMC S2/S3.

i The iRMC S2/S3 is supplied with a predefined server certificate (default certificate). If you want to access the iRMC S2/S3 over secure SSL/SSH connections, it is recommended that you replace the certificate with one signed by a Certificate Authority (CA) as soon as possible.

i Input format of the X.509 DSA/RSA certificate and the private DSA/RSA key:

The X.509 DSA/RSA certificate and the RSA/DSA must both be available in PEM-encoded format (ASCII/Base64).



Certificate Upload

Note: You may upload the contents of a base64 (PEM) encoded X.509 certificate and the matching DSA/RSA private key into the iRMC S2.
The maximum size for the base 64 (PEM) encoded private key is 4096 bytes.
The maximum size for the base 64 (PEM) encoded certificate is 6144 bytes.

Certificate Information and Restore

CA Certificate upload from file

Note: You may upload the contents of the base64 (PEM) encoded X.509 CA certificate from local file.
After you have uploaded the files, all current https connections will be closed and the https server will be automatically restarted. This can take up to 30seconds and **no** iRMC S2 reset is required.

CA Certificate file:

SSL Certificate and DSA/RSA private key upload from file

Note: You may upload the contents of the base64 (PEM) encoded X.509 certificate and the base64 (PEM) encoded DSA/RSA private key from local files.
Important: Both files need to be uploaded at the same time.
After you have uploaded the files, all current https connections will be closed and the https server will be automatically restarted. This can take up to 30seconds and **no** iRMC S2 reset is required.

SSL Private Key file:

SSL Certificate file:

SSL DSA/RSA certificate or DSA/RSA private key upload via copy & paste

Note: Alternatively you may paste the contents of the base64 (PEM) encoded X.509 SSL certificate **or** the base64 (PEM) encoded DSA/RSA private key into the textbox below for upload to the iRMC S2.
Important: Both files needs to be uploaded one after the other.
Important: Do not upload your CA certificate with this method into the iRMC S2. Use upload from file instead.
Important: After you have uploaded/pasted the file(s) in the textbox below, you need to restart the iRMC S2 manually.

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.

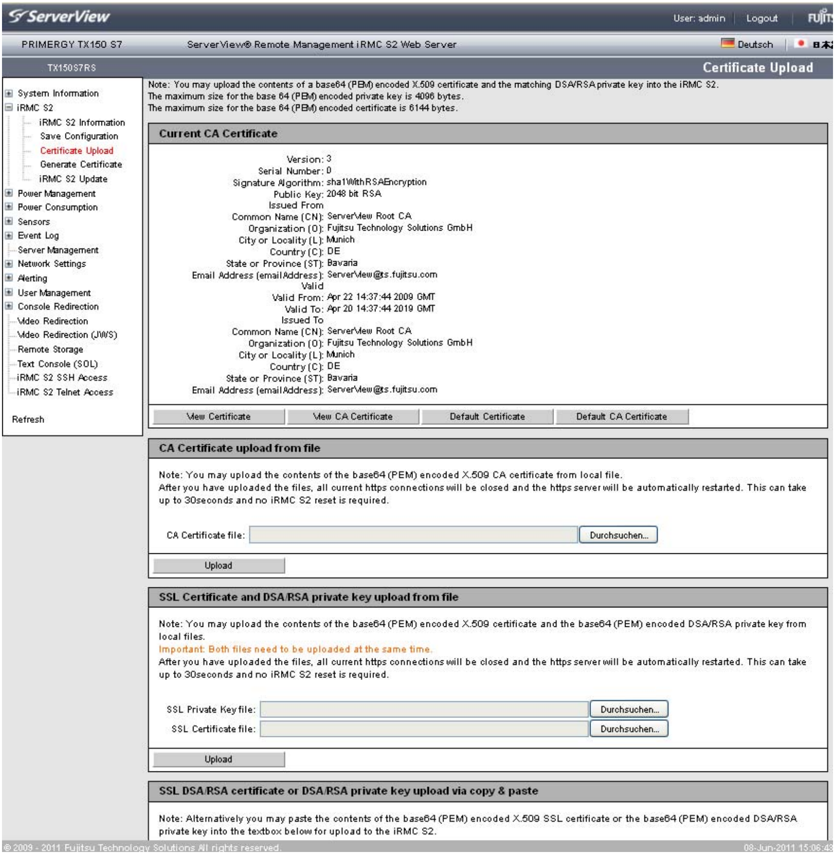
13-Jan 2011 17:17:57

Figure 88: Certificate Upload page

Displaying the currently valid (CA) DSA/RSA certificate

► In the group *Certificate Information and Restore*, click *View Certificate* to show the currently valid SSH/SSL-certificate.

► In the group *Certificate Information and Restore*, click *View CA Certificate* to show the currently valid CA certificate.



Note: You may upload the contents of a base64 (PEM) encoded X.509 certificate and the matching DSA/RSA private key into the iRMC S2.
The maximum size for the base 64 (PEM) encoded private key is 4096 bytes.
The maximum size for the base 64 (PEM) encoded certificate is 6144 bytes.

Current CA Certificate

Version: 3
Serial Number: 0
Signature Algorithm: sha1WithRSAEncryption
Public Key: 2048 bit RSA
Issued From
Common Name (CN): ServerView Root CA
Organization (O): Fujitsu Technology Solutions GmbH
City or Locality (L): Munich
Country (C): DE
State or Province (ST): Bavaria
Email Address (emailAddress): ServerView@ts.fujitsu.com
Valid
Valid From: Apr 22 14:37:44 2009 GMT
Valid To: Apr 20 14:37:44 2019 GMT
Issued To
Common Name (CN): ServerView Root CA
Organization (O): Fujitsu Technology Solutions GmbH
City or Locality (L): Munich
Country (C): DE
State or Province (ST): Bavaria
Email Address (emailAddress): ServerView@ts.fujitsu.com

CA Certificate upload from file

Note: You may upload the contents of the base64 (PEM) encoded X.509 CA certificate from local file.
After you have uploaded the files, all current https connections will be closed and the https server will be automatically restarted. This can take up to 30seconds and no iRMC S2 reset is required.

CA Certificate file:

SSL Certificate and DSA/RSA private key upload from file

Note: You may upload the contents of the base64 (PEM) encoded X.509 certificate and the base64 (PEM) encoded DSA/RSA private key from local files.
Important: Both files need to be uploaded at the same time.
After you have uploaded the files, all current https connections will be closed and the https server will be automatically restarted. This can take up to 30seconds and no iRMC S2 reset is required.

SSL Private Key file:
SSL Certificate file:

SSL DSA/RSA certificate or DSA/RSA private key upload via copy & paste

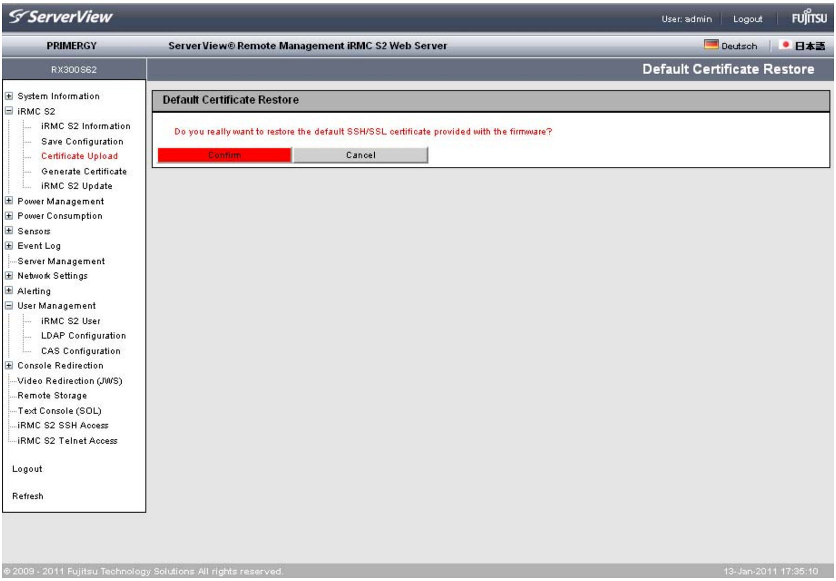
Note: Alternatively you may paste the contents of the base64 (PEM) encoded X.509 SSL certificate or the base64 (PEM) encoded DSA/RSA private key into the textbox below for upload to the iRMC S2.

Figure 89: Certificate Upload page - display of the currently valid SSL/SSH certificate

Restoring the default certificate default CA certificate

► In the group *Certificate Information and Restore*, click *Default Certificate* to restore the default certificate delivered with the firmware after you have confirmed that you wish to do so.

► In the group *Certificate Information and Restore*, click *Default CA Certificate* to restore the default CA certificate delivered with the firmware after you have confirmed that you wish to do so.



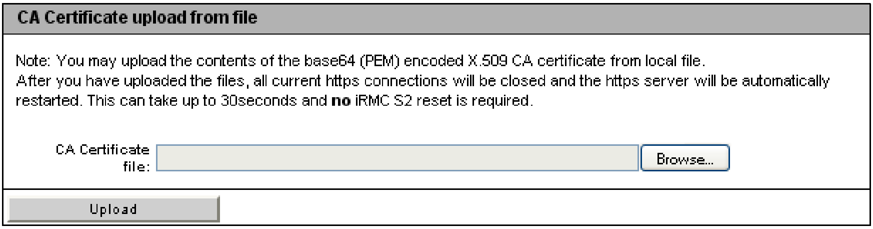
Default Certificate Restore

Do you really want to restore the default SSH/SSL certificate provided with the firmware?

Figure 90: Certificate Upload page - Restoring the default CA certificate

Loading a CA certificate from a local file

Use the *CA Certificate upload from file* group to load a CA certificate from a local file.



CA Certificate upload from file

Note: You may upload the contents of the base64 (PEM) encoded X.509 CA certificate from local file.
After you have uploaded the files, all current https connections will be closed and the https server will be automatically restarted. This can take up to 30seconds and **no** iRMC S2 reset is required.

Figure 91: Loading a CA certificate from a local file

Proceed as follows:

- Save the CA certificate in a local file on the managed server.
- Specify this file under *CA Certificate File* by clicking the associated *Browse...* button and navigating to the file containing the CA certificate.
- Click *Upload* to load the certificate and/or the private key onto the iRMC S2/S3.

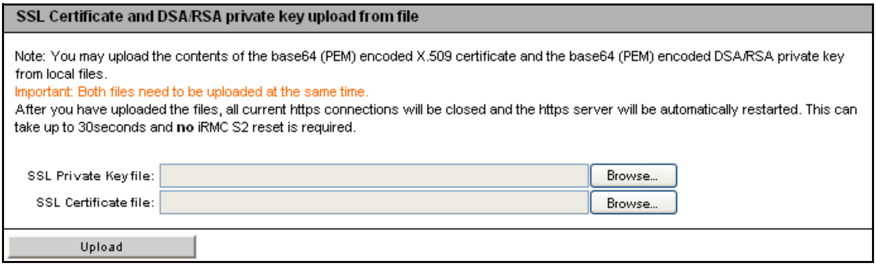
  i When you upload the certificate and/or private key, all the existing HTTPS connections are closed and the HTTPS server is automatically restarted. This process can take up to 30 seconds.

  No explicit reset of the iRMC S2/S3 is required.
- Click *View CA Certificate* to make sure that the certificate has been loaded successfully.

Loading the DSA/RSA certificate and private DSA/RSA key from local files

You do this using the group *SSL Certificate and DSA/RSA private key upload from file*.

i The private key and the certificate must be loaded on the iRMC S2/S3 at the same time.



SSL Certificate and DSA/RSA private key upload from file

Note: You may upload the contents of the base64 (PEM) encoded X.509 certificate and the base64 (PEM) encoded DSA/RSA private key from local files.
Important: Both files need to be uploaded at the same time.
After you have uploaded the files, all current https connections will be closed and the https server will be automatically restarted. This can take up to 30seconds and **no** iRMC S2 reset is required.

SSL Private Key file:
SSL Certificate file:

Figure 92: Loading the DSA/RSA certificate/private DSA/RSA key from local files

Proceed as follows:

- Save the X.509 DSA/RSA (SSL) certificate and the private DSA/RSA key in corresponding local files on the managed server.
- Specify the files *Private Key File* and *Certificate File* by clicking on the associated *Browse* button and navigating to the file which contains the private key or the certificate.
- Click *Upload* to load the certificate and the private key onto the iRMC S2/S3.

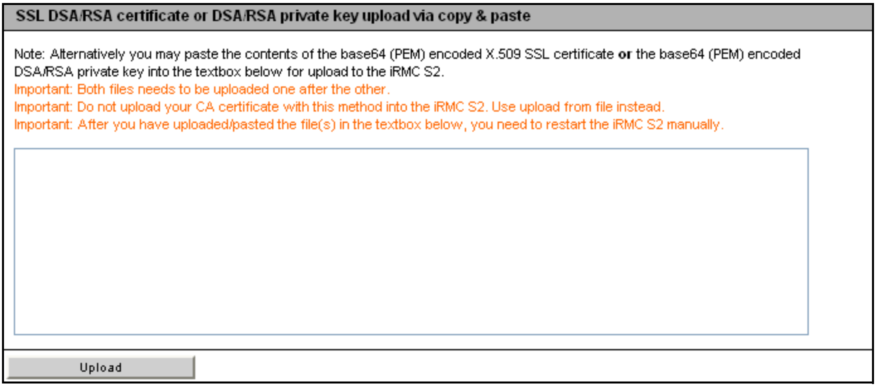
  i When you upload the certificate and private key, all the existing HTTPS connections are closed and the HTTPS server is automatically restarted. This process can take up to 30 seconds.

  No explicit reset of the iRMC S2/S3 is required.
- Click *View Certificate* to make sure that the certificate has been loaded successfully.

Entering the DSA/RSA certificate/private DSARSA key directly

You do this using the group *SSL DSA/RSA certificate or DSA/RSA private upload via copy & paste*.

Do **not** use this method to load a root certificate onto the iRMC S2/S3. Always load a root certificate using a file (see page 177).



SSL DSA/RSA certificate or DSA/RSA private key upload via copy & paste

Note: Alternatively you may paste the contents of the base64 (PEM) encoded X.509 SSL certificate **or** the base64 (PEM) encoded DSA/RSA private key into the textbox below for upload to the iRMC S2.
Important: Both files needs to be uploaded one after the other.
Important: Do not upload your CA certificate with this method into the iRMC S2. Use upload from file instead.
Important: After you have uploaded/pasted the file(s) in the textbox below, you need to restart the iRMC S2 manually.

Figure 93: Entering the DSA/RSA certificate/private DSARSA key directly

Proceed as follows:

- Copy the X.509 DSA certificate **or** the private DSA key to the input area.

  You cannot simultaneously enter the certificate and key for the same upload.

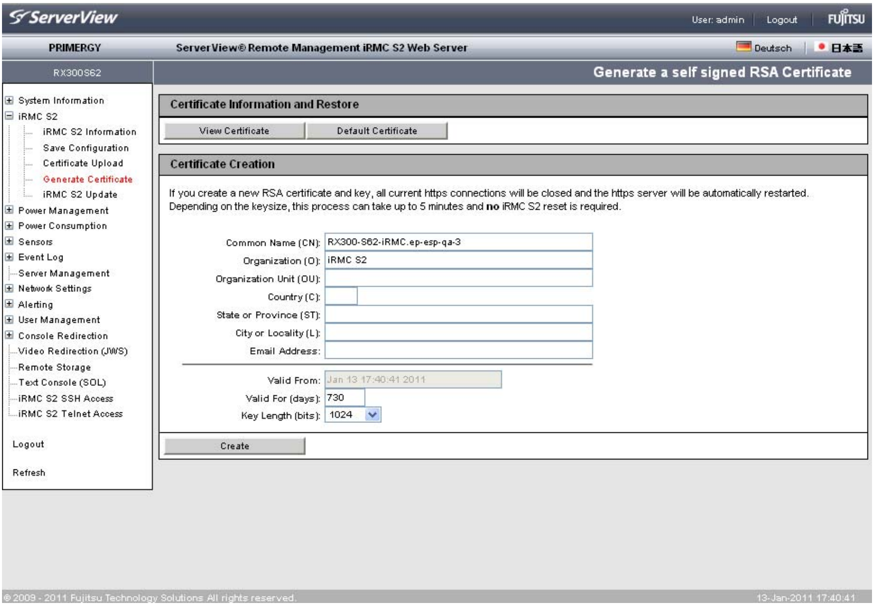
- Click *Upload* to load the certificate or the private key onto the iRMC S2/S3.
- Use the Remote Manager to reset the iRMC S2/S3 (see section "Service processor - IP parameters, identification LED and iRMC S2/S3 reset" on page 339).

  This is necessary in order to make a certificate or private key loaded onto the iRMC S2/S3 valid.

- Click *View Certificate* to make sure that the certificate has been loaded successfully.

7.6.4 Generate a self-signed Certificate - Generate self-signed RSA certificate

You can create a self-signed certificate using the *Generate a self-signed Certificate* page.



If you create a new RSA certificate and key, all current https connections will be closed and the https server will be automatically restarted. Depending on the keysize, this process can take up to 5 minutes and **no** iRMC S2 reset is required.

Common Name (CN): RX300-S62-iRMC.ep-esp-qa-3
Organization (O): iRMC S2
Organization Unit (OU):
Country (C):
State or Province (ST):
City or Locality (L):
Email Address:

Valid From: Jan 13 17:40:41 2011
Valid For (days): 730
Key Length (bits): 1024

Figure 94: Generate a self-signed RSA Certificate page

Certificate Information and Restore

The *Certificate Information and Restore* group allows you to view the currently valid DSA/RSA certificate and/or restore the default RSA/DSA certificate.

View Certificate
You can view the currently valid DSA/RSA certificate using this button.

Default Certificate
You can use this button to restore the default certificate delivered with the firmware after you have confirmed that you wish to do so.

Certificate Creation

Proceed as follows to create a self-signed certificate:

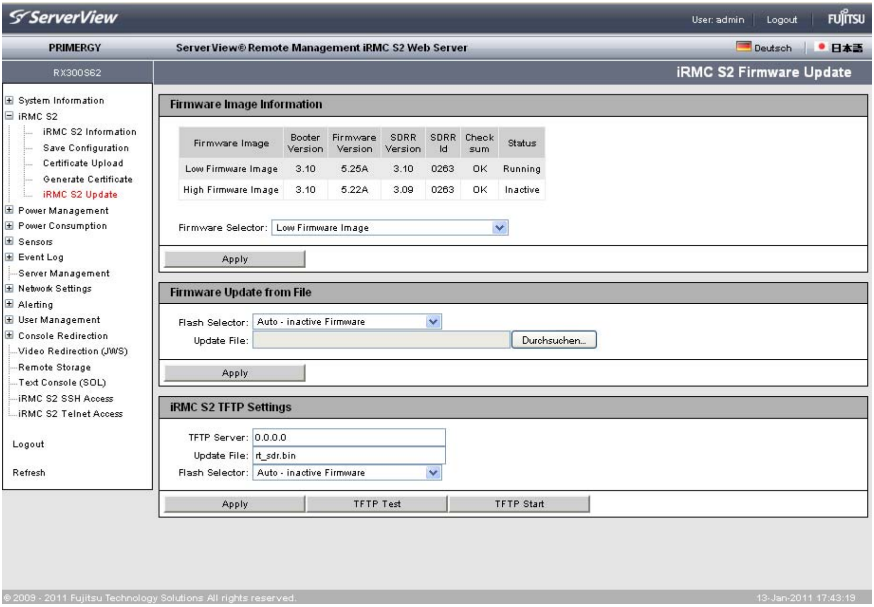
- Enter the requisite details under *Certificate Creation*.
- Click *Create* to create the certificate.

> When generating the new certificate, all the existing HTTPS connections are closed and the HTTPS server is automatically restarted. This can take up to 5 minutes depending on the key length.
>
> **No** explicit reset of the iRMC S2/S3 is required.

7.6.5 iRMC S2/S3 Firmware Update

The *iRMC S2/S3 Firmware Update* page allows you to update the iRMC S2/S3 firmware online. To do this, you must provide the current firmware image either locally on a remote workstation or on a TFTP server.

Here you can also see information on the iRMC S2/S3 firmware and set the firmware selector.



Firmware Image Information

Firmware Image	Booter Version	Firmware Version	SDRR Version	SDRR Id	Check sum	Status
Low Firmware Image	3.10	5.25A	3.10	0263	OK	Running
High Firmware Image	3.10	5.22A	3.09	0263	OK	Inactive

Firmware Selector: Low Firmware Image

Firmware Update from File

Flash Selector: Auto - inactive Firmware

Update File:

iRMC S2 TFTP Settings

TFTP Server: 0.0.0.0

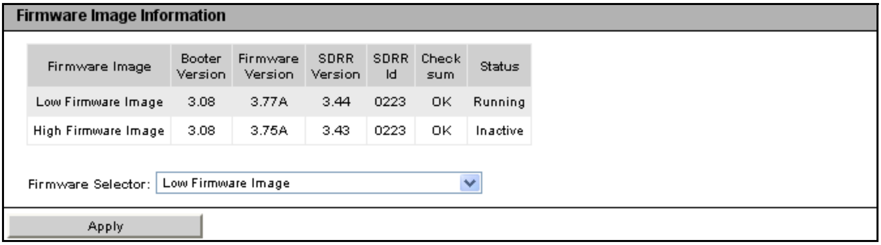
Update File: rt_sdr.bin

Flash Selector: Auto - inactive Firmware

Figure 95: iRMC S2/S3 Firmware Update page

Firmware Image Information

Under *Firmware Image Information*, you can view information on the firmware version and the SDRR version of the iRMC S2/S3 and set the firmware selector.



Firmware Image Information

Firmware Image	Booter Version	Firmware Version	SDRR Version	SDRR Id	Check sum	Status
Low Firmware Image	3.08	3.77A	3.44	0223	OK	Running
High Firmware Image	3.08	3.75A	3.43	0223	OK	Inactive

Firmware Selector: Low Firmware Image

Figure 96: iRMC S2/S3 Firmware Update - Firmware Information

Firmware Selector

You use the firmware selector to specify which firmware image is to be activated the next time the iRMC S2/S3 is rebooted.

You have the following options:

– *Auto - FW Image with highest FW version*

  The firmware image with the most recent version is selected automatically.

– *Low FW Image*

  The low firmware image is selected.

– *High FW Image*

  The high firmware image is selected.

– *Select FW Image with oldest FW version*

  The firmware image with the oldest version is selected.

– *Select most recently programmed FW*

  The most recently updated firmware image is selected.

– *Select least recently programmed FW*

  The least recently updated firmware image is selected.

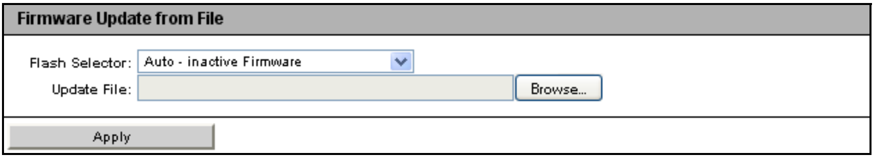
Apply

Click *Apply* to set the firmware selector to the option you have set under *Firmware Selector*.

Firmware Update from File

The *Firmware Update from File* group allows you to update the iRMC S2/S3 firmware online. To do this, you must provide the current firmware image in a file on a remote workstation.

You will find the appropriate firmware image for your PRIMERGY server on ServerView Suite DVD 1 or you can download it under *http://support.ts.fujitsu.com/com/support/downloads.html*.



Firmware Update from File

Flash Selector: Auto - inactive Firmware

Update File:

Figure 97: iRMC S2/S3 Firmware Update page - Firmware Update from File

Flash Selector

Specify what iRMC firmware is to be updated.

You have the following options:

– *Auto - inactive firmware*

  The inactive firmware is automatically selected.

– *Low Firmware Image*

  The low firmware image (firmware image 1) is selected.

– *High Firmware Image*

  The high firmware image (firmware image 2) is selected.

Update file

File in which the firmware image is stored.

> i The files listed below each allow you to update one component of the iRMC S2/S3 firmware in every update run (runtime firmware and SDR record).
>
> The file *rt_sdr_<D-number>_4_08g_00.bin* is also available for some PRIMERGY servers / blade servers. This allows you to update all the components of the iRMC S2/S3 firmware in a single operation.

dcod<FW-Version>.bin

Updates the runtime firmware.

<SDR-Version>.SDR

Updates the SDR record.

Browse...

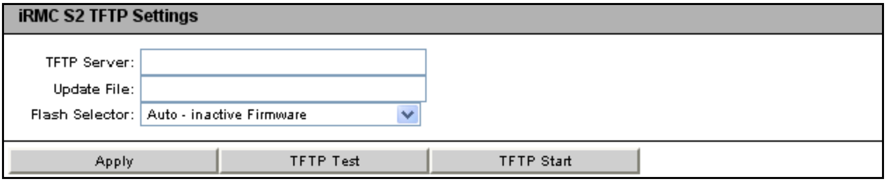
Opens a file browser that allows you to navigate to the update file.

► Click *Apply* to activate your settings and to start updating the iRMC S2/S3 firmware.

iRMC S2/S3 TFTP Settings

The *iRMC S2/S3 TFTP Settings* group allows you to update the iRMC S2/S3 firmware online. To do this, you must provide the current firmware image in a file on a TFTP server.

You will find the appropriate firmware image for your PRIMERGY server on ServerView Suite DVD 1 or you can download it under *http://support.ts.fujitsu.com/com/support/downloads.html*.



iRMC S2 TFTP Settings

TFTP Server:

Update File:

Flash Selector: Auto - inactive Firmware

Figure 98: iRMC S2/S3 Firmware Update page - iRMC S2/S3 TFTP Settings

TFTP Server

IP address or DNS name of the TFTP server on which the file with the firmware image is stored.

Update file

File in which the firmware image is stored.

> i The files listed below each allow you to update one component of the iRMC S2/S3 firmware every time TFTP is started (runtime firmware and SDR record).
>
> The file *rt_sdr_<D-number>_4_08g_00.bin* is also available for some PRIMERGY servers / blade servers. This allows you to update all the components of the iRMC S2/S3 firmware in a single operation using a TFTP server.

dcod<FW-Version>.bin

Updates the runtime firmware.

<SDR-Version>.SDR

Updates the SDR record.

Flash Selector

Specify what iRMC firmware is to be updated.

You have the following options:

- *Auto - inactive firmware*

  The inactive firmware is automatically selected.

- *Low Firmware Image*

  The low firmware image (firmware image 1) is selected.

- *High Firmware Image*

  The high firmware image (firmware image 2) is selected.

- ► Click *Apply* to activate your settings.
- ► Click *TFTP Test* to test the connection to the TFTP server.
- ► Click *TFTP Start* to download the file containing the firmware image from the TFTP server and to start updating the iRMC S2/S3 firmware.

7.7 Power Management

The *Power Management* entry contains the links to the power management pages for your PRIMERGY server:

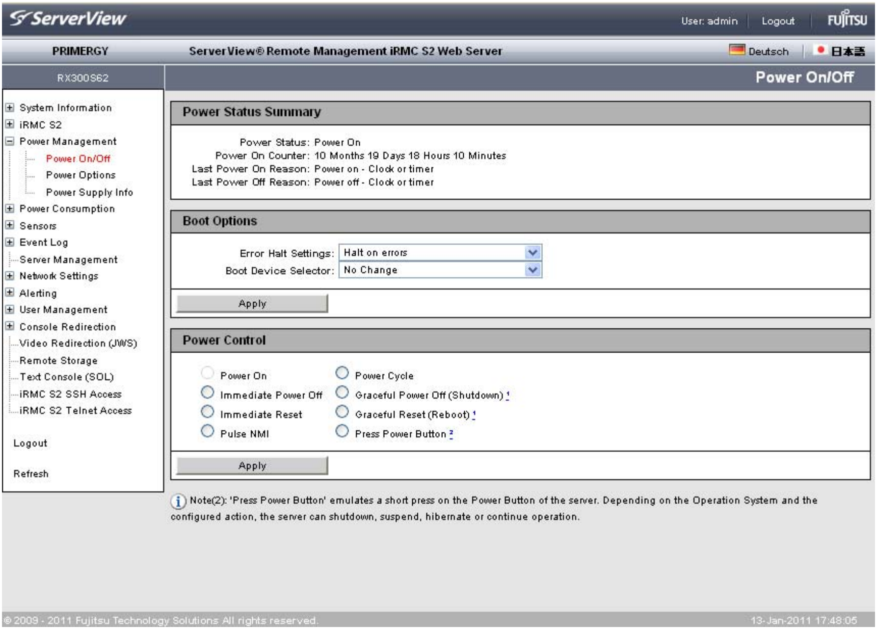
– "Power On/Off - power the server up/down" on page 187.

– "Power Options - Configuring power management for the server" on page 191.

– "Power Supply Info - Power supply and IDPROM data for the FRU components" on page 198.

7.7.1 Power On/Off - power the server up/down

The *Power On/Off* page allows you to power the managed server on and off. You are informed of the server's current power status and are also able to configure the behavior of the server during the next boot operation.



Power Status Summary

Power Status: Power On
Power On Counter: 10 Months 19 Days 18 Hours 10 Minutes
Last Power On Reason: Power on - Clock or timer
Last Power Off Reason: Power off - Clock or timer

Boot Options

Error Halt Settings: Halt on errors
Boot Device Selector: No Change

Power Control

○ Power On ○ Power Cycle
○ Immediate Power Off ○ Graceful Power Off (Shutdown) 1
○ Immediate Reset ○ Graceful Reset (Reboot) 1
○ Pulse NMI ○ Press Power Button 2

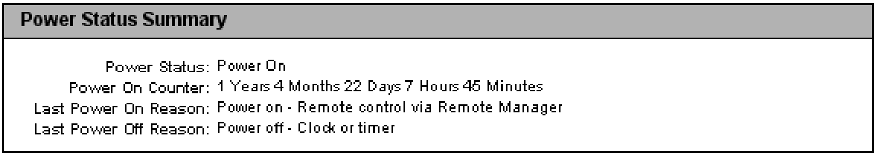
Note(2): 'Press Power Button' emulates a short press on the Power Button of the server. Depending on the Operation System and the configured action, the server can shutdown, suspend, hibernate or continue operation.

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved. 13-Jan-2011 17:48:05

Figure 99: Power On/Off page

Power Status Summary

The *Power Status Summary* group provides information on the current power status of the server and on the causes for the most recent Power On/Power Off. In addition, a Power On counter records the total months, days and minutes during which the server has been powered.



Power Status Summary

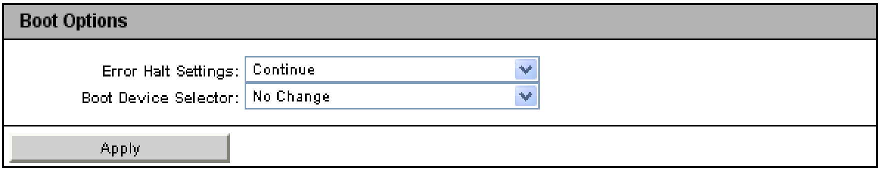
Power Status: Power On
Power On Counter: 1 Years 4 Months 22 Days 7 Hours 45 Minutes
Last Power On Reason: Power on - Remote control via Remote Manager
Last Power Off Reason: Power off - Clock or timer

Figure 100: Power On/Off page - Power Status Summary

Boot Options

The *Boot Options* group allows you to configure the behavior of the system the **next** time it is booted. You can set whether the BIOS is to interrupt the boot process for the system if errors occur during the POST phase.

The options set here only apply to the next boot operation. After this, the default mechanism applies again.



Boot Options

Error Halt Settings: Continue

Boot Device Selector: No Change

Figure 101: Power Management - Boot Options page

► Select the desired BIOS behavior from the *Error Halt Settings* list:

Continue
Continue the boot process if errors occur during the POST phase.

Halt on errors
Interrupt the boot process if errors occur during the POST phase.

► From the *Boot Device Selector* list, select the storage medium you wish to boot from.

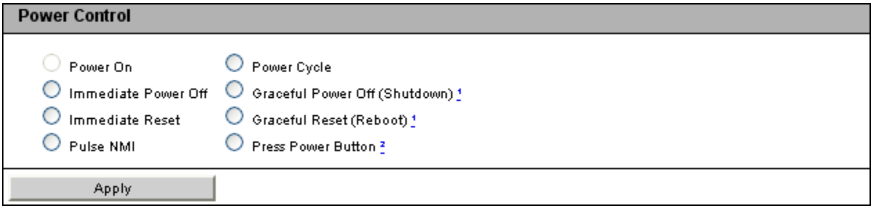
The following options are available:

- *No change*: The system is booted from the same storage medium as previously.
- *PXE/iSCSI*: The system is booted from PXE/iSCSI over the network.
- *Harddrive*: The system is booted from hard disk.
- *CDROM/DVD*: The system is booted from CD /DVD.
- Floppy: The system is booted from floppy disk.

► Click *Apply* to activate your settings.

Power Control - powering the server up and down/rebooting the server

The *Power Control* group allows you to power the server up/down or to reboot the server.



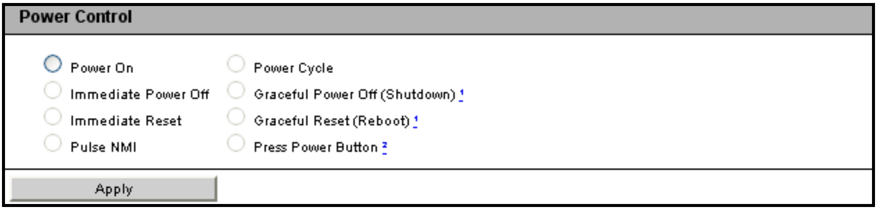
Power Control

○ Power On
○ Immediate Power Off
○ Immediate Reset
○ Pulse NMI

○ Power Cycle
○ Graceful Power Off (Shutdown) [1]
○ Graceful Reset (Reboot) [1]
○ Press Power Button [2]

Apply

Figure 102: Power On/Off page, Restart (server is powered up)



Power Control

○ Power On
○ Immediate Power Off
○ Immediate Reset
○ Pulse NMI

○ Power Cycle
○ Graceful Power Off (Shutdown) [1]
○ Graceful Reset (Reboot) [1]
○ Press Power Button [2]

Apply

Figure 103: Power On/Off page, Restart (server is powered down)

Power On

Switches the server on.

Immediate Power Off

Powers the server down, regardless of the status of the operating system.

Immediate Reset

Completely restarts the server (cold start), regardless of the status of the operating system.

Pulse NMI

Initiates a non-maskable interrupt (NMI). A NMI is a processor interrupt that cannot be ignored by standard interrupt masking techniques in the system.

Press Power Button

Depending on the operating system installed and the action configured, you can trigger various actions by briefly pressing the power-off button. These actions could be shutting down the computer or switching it to standby mode or sleep mode.

Power Cycle

Powers the server down completely and then powers it up again after a configured period. You can configure this time in the *Power Cycle Delay* field of the *ASR&R Options* group (see page 234).

Graceful Power Off (Shutdown)

Graceful shutdown and power off.
This option is only available if ServerView agents are installed and signed onto the iRMC S2/S3 as “Connected”.

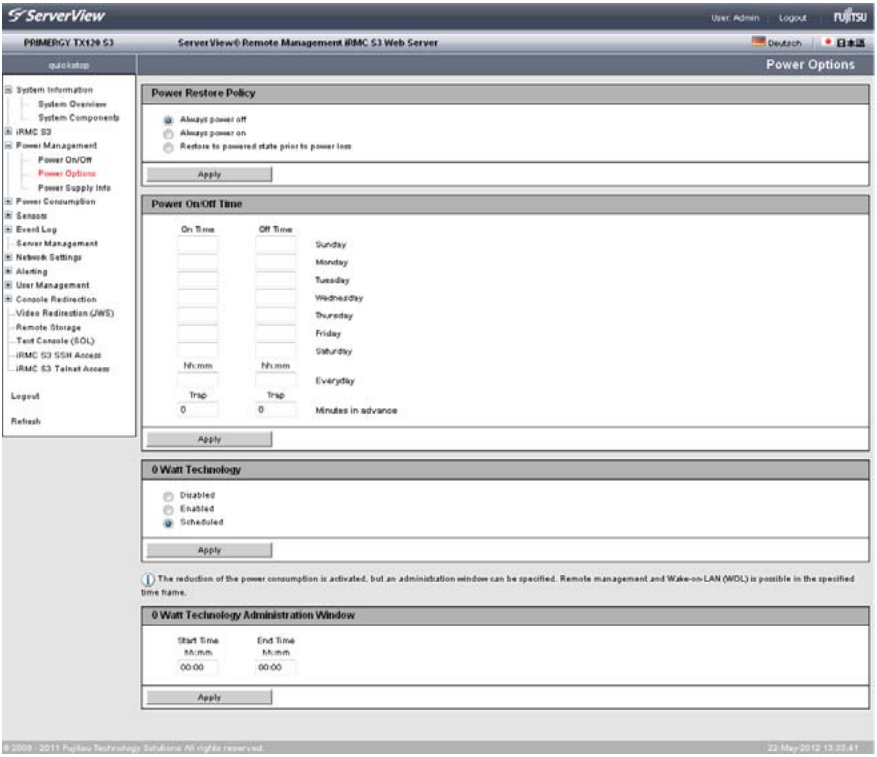
Graceful Reset (Reboot)

Graceful shutdown and reboot.
This option is only available if ServerView agents are installed and signed onto the iRMC S2/S3 as “Connected”.

► Click *Apply* to start the required action.

7.7.2 Power Options - Configuring power management for the server

The *Power Options* page allows you to define the server’s behavior after a power outage and specify the server’s power on/off times.



Power Restore Policy

- ● Always power off
- ○ Always power on
- ○ Restore to powered state prior to power loss

Power On/Off Time

On Time	Off Time	
		Sunday
		Monday
		Tuesday
		Wednesday
		Thursday
		Friday
		Saturday
hh:mm	hh:mm	
		Everyday
Trap	Trap	
0	0	Minutes in advance

0 Watt Technology

- ○ Disabled
- ○ Enabled
- ● Scheduled

The reduction of the power consumption is activated, but an administration window can be specified. Remote management and Wake-on-LAN (WOL) is possible in the specified time frame.

0 Watt Technology Administration Window

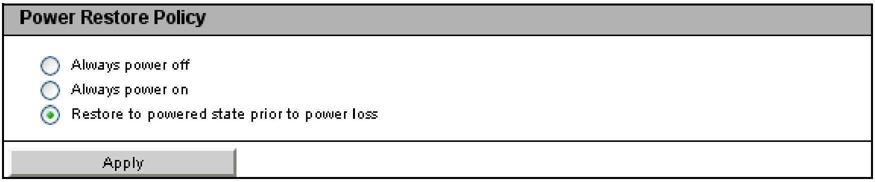
Start Time hh:mm	End Time hh:mm
00:00	00:00

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.
22-May-2012 13:33:41

Figure 104: Power Options page

Power Restore Policy - Specify behavior of the server after a power outage

The *Power Restore Policy* group allows you to specify the server’s power management behavior after a power outage.



Power Restore Policy

○ Always power off
○ Always power on
● Restore to powered state prior to power loss

Figure 105: Power Options page, Power Restore Policy

Always power off
: The server always remains powered down after a power outage.

Always power on
: The server is always powered up again after a power outage.

Restore to powered state prior to power loss
: The power up/down status of the server is restored to the status prior to the power outage.

- ► Click *Apply* to activate your settings.

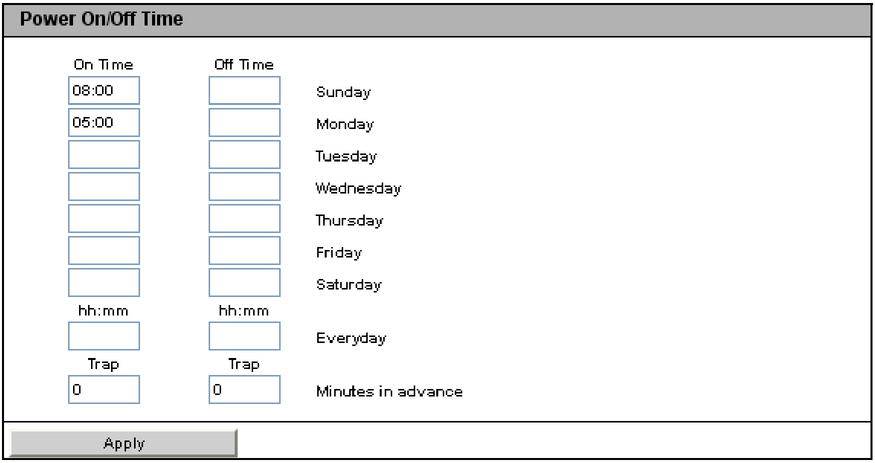
The configured action will be performed after a power outage.

Power On/Off Time - Specify power on/off times for the server

The input fields of the *Power On/Off Time* group allow you to specify the times at which the server is powered up/down for the individual days of the week or for specified times during the day.

Specifications in the *Everyday* field take priority!

The *Trap* fields also allow you to configure whether the iRMC S2/S3 sends an SNMP trap to the management console before a planned power-on / power-off of the managed server and, if so, how many minutes before the event this should be done. No traps are sent if you specify the value “0”.



Power On/Off Time

On Time	Off Time	
08:00		Sunday
05:00		Monday
		Tuesday
		Wednesday
		Thursday
		Friday
		Saturday
hh:mm	hh:mm	
		Everyday
Trap	Trap	
0	0	Minutes in advance

Figure 106: Power Options page, Power On/Off Time

0 Watt Technology

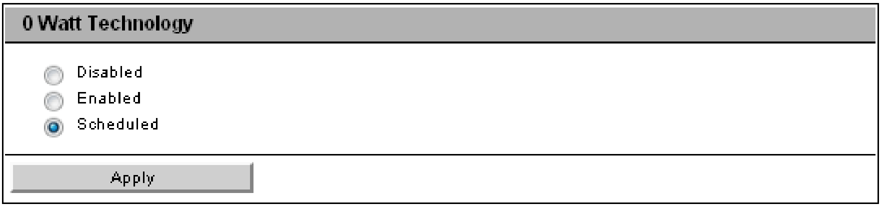
Please note:

- This feature is only supported by the iRMC S3.
- This feature is not supported for all PRIMERGY servers.

The "0 Watt Technology" feature allows you to reduce the server’s standby power consumption to 0 watts. Every time the server is powered off, the server’s standby power consumption is reduced to 0 Watt (*0 Watt* mode).

In the *0 Watt* mode, the server can no longer be managed remotely. The server can only be powered on by pressing the *Power* button or the *PSU Primary Resume* button.

However, by applying the *Scheduled* option (see page 196) you can specify a time interval at which the PSU is awoken from *0 Watt* mode and thus both remote management and Wake-on-LAN (WOL) can be used.



0 Watt Technology

○ Disabled
○ Enabled
● Scheduled

Figure 107: Power Options page, 0 Watt Technology

Disabled

Disables *0 Watt* mode and remains in / switches to the standard power on/off mode. The server can be managed remotely at any time.

Enabled

Enables *0 Watt* mode.

Even if *Enabled* has been configured, the *0 Watt* mode is blocked in the following cases:

- Power-cycle request / power-on delay

  A power cycle request powers down the server without enabling *0 Watt* mode, i.e. *0 Watt* mode will not be enabled in the delay between powering down and powering up during a power cycle:

  – Any power-on request occurring within the delay causes the server to be powered on after the delay is over.

  – If no power-on request occurred during the delay, the iRMC S3 enables the *0 Watt* mode after the delay time period has passed.

- Thermal power-on prohibition

  If the *Temperature Monitoring* mode (system thermal power on prohibition) has been configured in the BIOS/UEFI setup menu, *0 Watt* mode will not be enabled.

- ASR&R

  Any ASR&R action currently reducing the retry counter prevents *0 Watt* mode from being enabled. This applies even if the server was finally powered off after the retry counter reached 0.

- Scheduled *Power On/Off Time* (see "Power On/Off Time - Specify power on/off times for the server" on page 193)

  As long as a *Power On/Off* timer configured in the iRMC S3 *Power Options* page is active, *0 Watt* mode cannot be enabled.

  0 Watt mode also cannot be enabled if the *Power On/Off* timer gets deactivated while the server is powered off. In this case, only next power-off transition will enable *0 Watt* mode. No scheduled *Power On/Off* timer will then prevent *0 Watt* mode from being enabled.

- Global Error LED

  If the global Error LED indicates any problematic system health conditions, the iRMC S3 will not enable *0 Watt* mode. This is because the server must be able to report system health problems even if powered off.

- System Identification LED

  As long as the System Identification LED is on, the iRMC S3 will not enable *0 Watt* mode.

- Advanced Video Redirection (AVR)

  If an AVR session is currently active, the iRMC S3 will not enable *0 Watt* mode. Once all AVR sessions have been finished (i.e, no AVR is active), the iRMC S3 will enable *0 Watt* mode.

- Remote Storage Server (RSS), Telnet/SSH Sessions

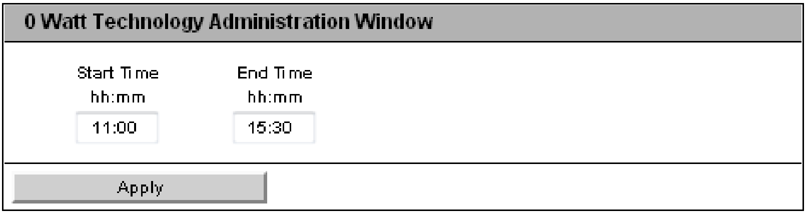
  If an RSS session or an SSH/Telnet session is currently active, the iRMC S3 will not enable *0 Watt* mode. This prevents the remote interface connections to the iRMC S3 from being lost.

- AC power fail

  If an AC fail occurs and the PSU (Power Supply Unit) is in the *0 Watt* mode or in the scheduled mode, the PSU will return to system standby. Depending on the power restore policy settings (see page 192), the iRMC S3 determines whether the server is to be powered on. If the power restore policy is set to *Always power off*, an AC fail will never result in *0 Watt* mode. *0 Watt* mode may be reached after the next system power on.

Scheduled

Enables *0 Watt* mode and also displays the *0 Watt Technology Administration Window*. The *0 Watt Technology Administration Window* allows you to specify a time interval at which the PSU is awoken from *0 Watt* mode and thus both remote management and Wake-on-LAN (WOL) can be used.



0 Watt Technology Administration Window

Start Time hh:mm: 11:00

End Time hh:mm: 15:30

Figure 108: Power Options page, 0 Watt Technology Administration window

Start Time

Defines the beginning (*hh:mm*) of the time interval.

End Time

Defines the end (*hh:mm*) of the time interval.

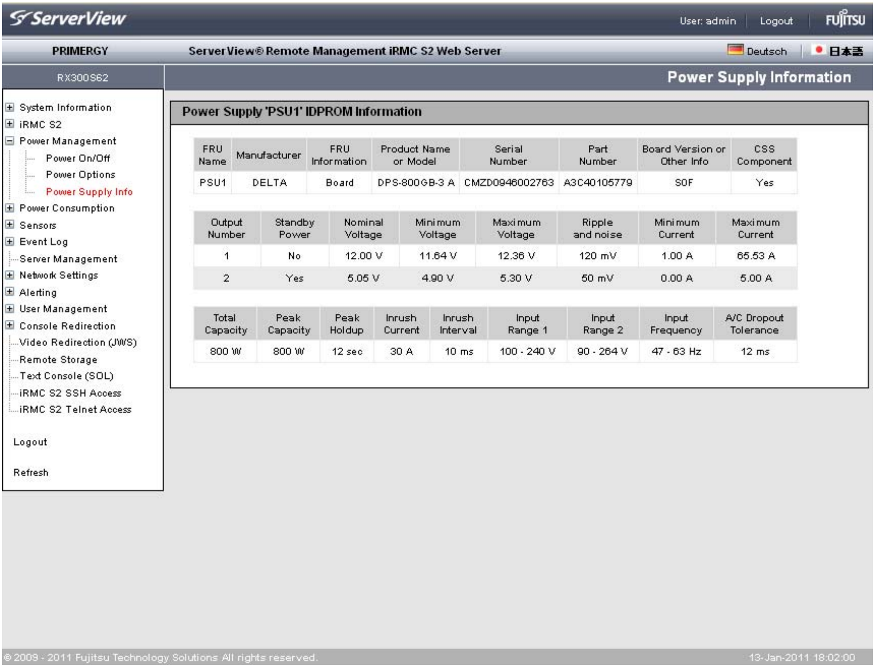
- ► Click *Apply* to activate your settings.

► Click *Apply* to activate your settings.

7.7.3 Power Supply Info - Power supply and IDPROM data for the FRU components

The *Power Supply Info* page provides you with information on the power supply specifications and the IDPROM data of the FRUs of the server.

The *CSS Component* column indicates for each of the components whether the CSS (**C**ustomer **S**elf **S**ervice) functionality is supported.



Power Supply 'PSU1' IDPROM Information

FRU Name	Manufacturer	FRU Information	Product Name or Model	Serial Number	Part Number	Board Version or Other Info	CSS Component
PSU1	DELTA	Board	DPS-800GB-3 A	CMZD0946002763	A3C40105779	S0F	Yes

Output Number	Standby Power	Nominal Voltage	Minimum Voltage	Maximum Voltage	Ripple and noise	Minimum Current	Maximum Current
1	No	12.00 V	11.64 V	12.36 V	120 mV	1.00 A	65.53 A
2	Yes	5.05 V	4.90 V	5.30 V	50 mV	0.00 A	5.00 A

Total Capacity	Peak Capacity	Peak Holdup	Inrush Current	Inrush Interval	Input Range 1	Input Range 2	Input Frequency	A/C Dropout Tolerance
800 W	800 W	12 sec	30 A	10 ms	100 - 240 V	90 - 264 V	47 - 63 Hz	12 ms

Figure 109: Power Supply Info page

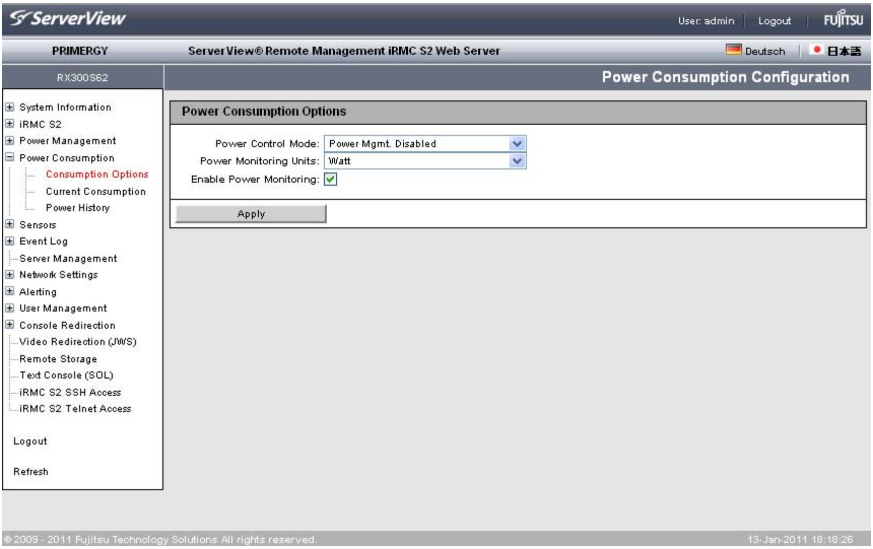
7.8 Power Consumption

The *Power Consumption* entry contains the links to the pages for monitoring and controlling the power consumption of the managed server:

- "Power Consumption Configuration - Configure power consumption of the server" on page 200.
- "Power Options - Configuring power management for the server" on page 191. (Not shown on all servers with iRMC S2/S3.)
- "Power Consumption History - Show server power consumption" on page 207 (Not shown on all servers with iRMC S2/S3.)

7.8.1 Power Consumption Configuration - Configure power consumption of the server

The *Power Consumption Configuration* page allows you to specify the mode the iRMC S2/S3 uses to control the power consumption of your PRIMERGY server.



Power Consumption Configuration

Power Consumption Options

Power Control Mode: Power Mgmt. Disabled

Power Monitoring Units: Watt

Enable Power Monitoring: ☑

Figure 110: Power Consumption Configuration page

Prerequisite:

The following requirements must be met in order to configure power consumption control:

– The managed PRIMERGY server must support this feature.

– The *Enhanced Speed Step* or the *Processor Power Management* option must be enabled in the *Advanced* Menu of the BIOS setup.

If you set the “Power Limit” power control mode in the *Power Consumption Options* group or in the S*cheduled Power Consumption Configuration*, the *Power Limit Options* group is also displayed (see page 202).

Power Consumption Options

The *Power Consumption Options* group allows you to select the power control mode and specify whether the power consumption should be monitored over time.

Power Control Mode

Mode for controlling the power consumption of the managed server:

- *Power Mgmt. Disabled*:

  The iRMC S2/S3 allows the operating system to control power consumption.

- *Best Performance*:

  The iRMC S2/S3 controls the server to achieve best performance. In this event, power consumption can rise.

- *Low Noise*: (iRMC S3 only)

  The iRMC S3 controls the server to achieve the lowest possible noise emission. This feature is not supported for all PRIMERGY servers and only available for specific configurations.

- *Minimum Power*:

  The iRMC S2/S3 controls the server to achieve the lowest possible power consumption. In this event, performance is not always ideal.

- *Power Limit*:

  The *Power Limit Options* group is displayed (see "Power Limit Options" on page 204).

- *Scheduled*:

  The iRMC S2/S3 controls power consumption in accordance with a schedule that you can define using the SCU (see "Scheduled Power Consumption Configuration" on page 202).

Power Monitoring Units

Unit of electrical power used to display power consumption:

- *Watt*
- *BTU/h* (British Thermal Unit/hour, 1 BTU/h corresponds to 0.293 Watt).

Enable Power Monitoring

If you enable this option, power consumption is monitored over time.

i Power monitoring is enabled by default as of Version 3.32 of the firmware.

i This setting only takes effect on PRIMERGY servers that support power monitoring.

► Click *Apply* to activate your settings.

Scheduled Power Consumption Configuration

The *Scheduled Power Consumption Configuration* group allows you to specify in detail the schedules and modes (operating-system-controlled, best performance, lowest power consumption) that the iRMC S2/S3 uses to control power consumption on the managed server.

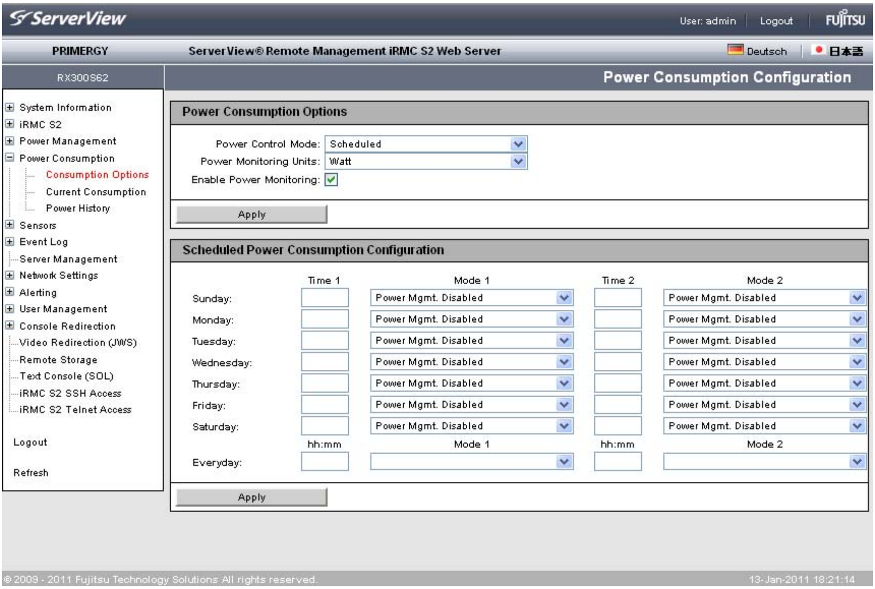
i The *Scheduled Power Consumption Configuration* group only appears if you have enabled the power control mode *scheduled* in the *Power Consumption Options* group.

i Configuration for scheduled power control mode assumes that the *Enhanced Speed Step* option has been enabled in the BIOS setup. If this is not the case, a message to this effect is displayed.

If this message appears even though “Enhanced Speed Step” is enabled, this may be because:

– The CPU (e.g. low-power CPU) of the server does not support scheduled power control.

– The system is currently in the BIOS POST phase.



Power Consumption Configuration

Power Consumption Options

Power Control Mode: Scheduled

Power Monitoring Units: Watt

Enable Power Monitoring: ☑

Scheduled Power Consumption Configuration

	Time 1	Mode 1	Time 2	Mode 2
Sunday:		Power Mgmt. Disabled		Power Mgmt. Disabled
Monday:		Power Mgmt. Disabled		Power Mgmt. Disabled
Tuesday:		Power Mgmt. Disabled		Power Mgmt. Disabled
Wednesday:		Power Mgmt. Disabled		Power Mgmt. Disabled
Thursday:		Power Mgmt. Disabled		Power Mgmt. Disabled
Friday:		Power Mgmt. Disabled		Power Mgmt. Disabled
Saturday:		Power Mgmt. Disabled		Power Mgmt. Disabled
	hh:mm	Mode 1	hh:mm	Mode 2
Everyday:				

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.

13-Jan-2011 18:21:14

Figure 111: Power Consumption Configuration page (scheduled)

Time 1

Time [hh:ss] at which the iRMC S2/S3 starts power control as defined in *Mode 1* on the relevant day of the week.

Time 2

Time [hh:ss] at which the iRMC S2/S3 starts power control as defined in *Mode 2* on the relevant day of the week.

Mode 1

Power consumption mode used by the iRMC S2/S3 for power control as of *Time 1* on the relevant day of the week.

Mode 2

Power consumption mode used by the iRMC S2/S3 for power control as of *Time 2* on the relevant day of the week.

i Set *Time 1* < *Time 2*, otherwise the power control mode specified under *Mode 2* will only be activated at *Time 2* on the relevant day of the following week.

i Specifications in the *Everyday* field take priority.

► Click *Apply* to activate your settings.

> i You can also configure scheduled power control using the Server Configuration Manager (see chapter "Configuring iRMC S2/S3 using the Server Configuration Manager" on page 347).

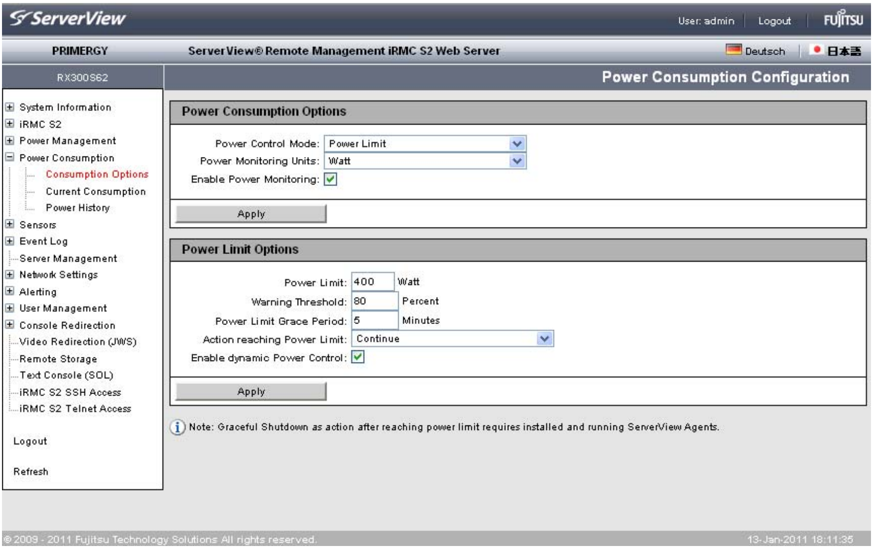
Power Limit Options

The *Power Limit Options* group is displayed under the following circumstances:

– The power control mode *Power Limit* is selected and enabled in the *Power Consumption Options* group.

– The power control mode *Scheduled* is enabled in the *Power Consumption Options* group and the power control mode *Power Limit* is enabled at least once in the *Scheduled Power Consumption Configuration* group.

  The power limit then applies to all periods for which this power control mode is enabled in the *Scheduled Power Consumption Configuration* group.



Power Consumption Options

Power Control Mode: Power Limit
Power Monitoring Units: Watt
Enable Power Monitoring: ☑

Power Limit Options

Power Limit: 400 Watt
Warning Threshold: 80 Percent
Power Limit Grace Period: 5 Minutes
Action reaching Power Limit: Continue
Enable dynamic Power Control: ☑

Note: Graceful Shutdown as action after reaching power limit requires installed and running ServerView Agents.

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved. 13-Jan-2011 18:11:35

Figure 112: Power Consumption Configuration page (scheduled)

Power Limit
  Maximum power consumption (in Watts).

Warning Threshold

Threshold as a percentage of the maximum power consumption specified under *Power Limit*. When the threshold is reached, the action defined under *Action Reaching Power Limit* is performed.

Power Limit Grace Period

Period (in minutes) for which the system waits after the threshold has been reached until the action is performed.

Action Reaching Power Limit

Action to be performed after the threshold has been reached and the grace period has expired.

Continue

No action is performed.

Graceful Power Off (Shutdown)

Shut down the system "gracefully" and power it down.

i This option is only supported if ServerView agents are installed and signed onto the iRMC S2/S3 as “Connected”.

Immediate Power Off

The server is immediately powered down irrespective of the status of the operating system.

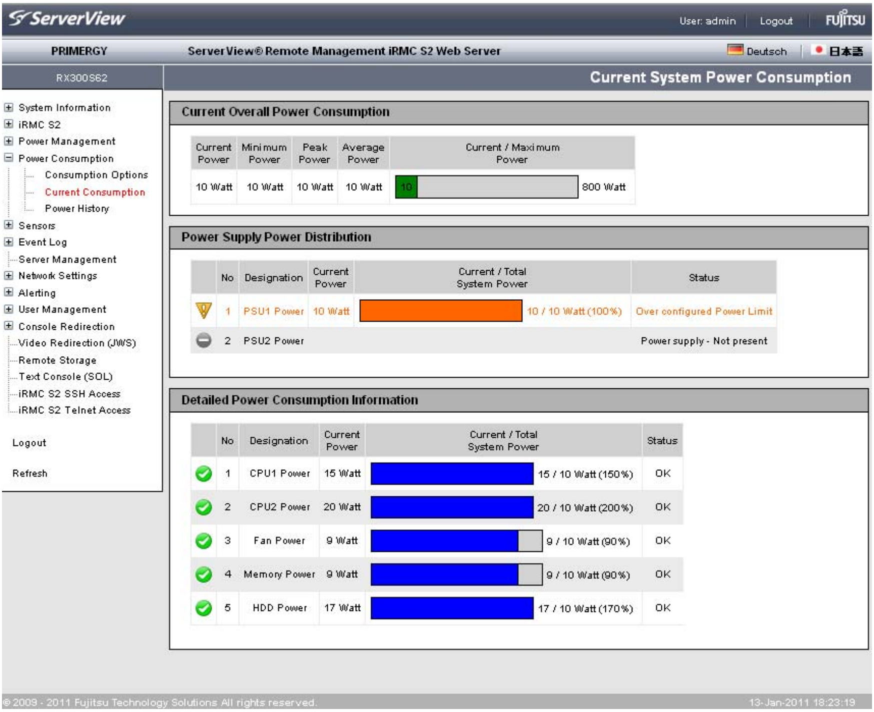
Enable Dynamic Power Control

The power limit is controlled dynamically. If this option is enabled, the iRMC S2/S3 controls the power consumption of the server system by reducing the CPU’s power consumption as soon as the *Warning Threshold* is reached.

7.8.2 Current Power Consumption - Show the current power consumption

> This view is not supported by all PRIMERGY servers with iRMC S2/S3.

The *Current Power Consumption* page shows the current power consumption of the system components and of the overall system.



Current Overall Power Consumption

Current Power	Minimum Power	Peak Power	Average Power	Current / Maximum Power
10 Watt	10 Watt	10 Watt	10 Watt	10 800 Watt

Power Supply Power Distribution

	No	Designation	Current Power	Current / Total System Power	Status
⚠	1	PSU1 Power	10 Watt	10 / 10 Watt (100%)	Over configured Power Limit
⊖	2	PSU2 Power			Power supply - Not present

Detailed Power Consumption Information

	No	Designation	Current Power	Current / Total System Power	Status
✓	1	CPU1 Power	15 Watt	15 / 10 Watt (150%)	OK
✓	2	CPU2 Power	20 Watt	20 / 10 Watt (200%)	OK
✓	3	Fan Power	9 Watt	9 / 10 Watt (90%)	OK
✓	4	Memory Power	9 Watt	9 / 10 Watt (90%)	OK
✓	5	HDD Power	17 Watt	17 / 10 Watt (170%)	OK

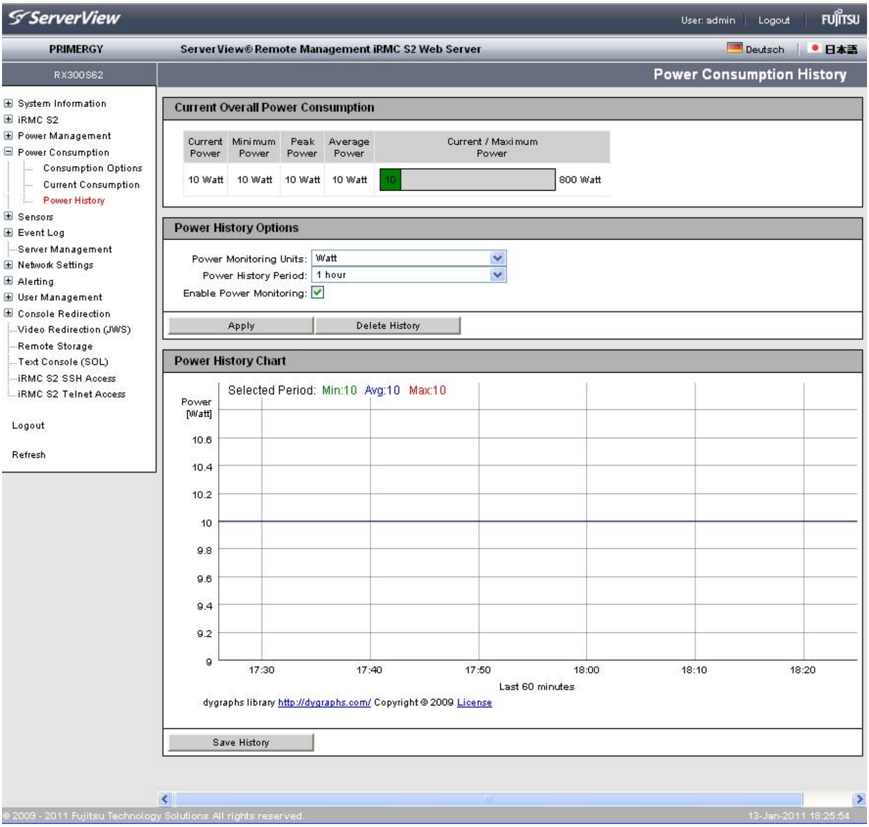
© 2009 - 2011 Fujitsu Technology Solutions All rights reserved. 13-Jan-2011 18:23:19

Figure 113: Current Power Consumption page

7.8.3 Power Consumption History - Show server power consumption

The *Power Consumption History* page charts the power consumption of your PRIMERGY server.

> **i** This page is not shown on all PRIMERGY servers with iRMC S2/S3.



Current Overall Power Consumption

Current Power	Minimum Power	Peak Power	Average Power	Current / Maximum Power	
10 Watt	10 Watt	10 Watt	10 Watt	10	800 Watt

Power History Options

Power Monitoring Units: Watt

Power History Period: 1 hour

Enable Power Monitoring: ☑

Power History Chart

Selected Period: Min:10 Avg:10 Max:10

dygraphs library http://dygraphs.com/ Copyright © 2009 License

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.

13-Jan-2011 18:25:54

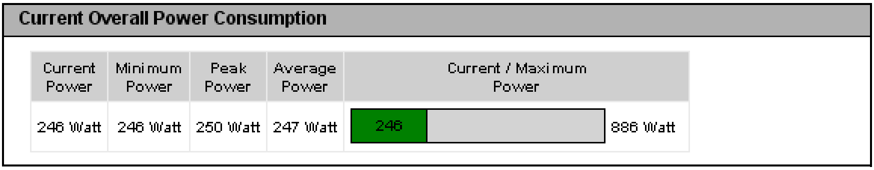
Figure 114: Power Consumption History page

Current Power Consumption

This option is not supported for all PRIMERGY servers.

Under *Current Power Consumption* you can see all the measurements for the server power consumption in the current interval: current, minimum, maximum and average power consumption.

A graphical display also shows the current power consumption of the server compared with the maximum possible power consumption.



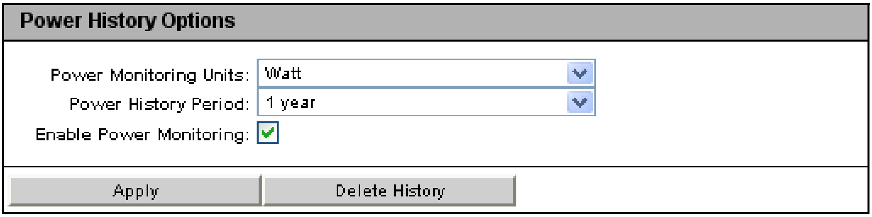
Current Overall Power Consumption

Current Power	Minimum Power	Peak Power	Average Power	Current / Maximum Power	
246 Watt	246 Watt	250 Watt	247 Watt	246	886 Watt

Figure 115: Power Consumption History - Current Power Consumption

Power History Options

You specify the parameters for displaying the power consumption under Power History Options.



Power History Options

Power Monitoring Units: Watt

Power History Period: 1 year

Enable Power Monitoring: ☑

Figure 116: Power Consumption History - Power History Options

Power History Units

Electrical power units:

- Watt
- *BTU/h* (British Thermal Unit/hour, 1 BTU/h corresponds to 0.293 Watt).

Power History Period

Period for which the power consumption is charted.

The following intervals can be selected:

1 hour

Default.
Measurements for the last hour (60 values). Since one measurement is generated every minute, this shows all the measurements of the last hour.

12 hours

Measurements for the last 12 hours. One measurement is shown for each five-minute period (every 5th measurement, 144 values in all).

1 day

Measurements for the last 24 hours. One measurement is shown for each 10-minute period (every 10th measurement, 144 values in all).

1 week

The measurements for the last week. One measurement per hour is shown (every 60th measurement, 168 values in all).

2 weeks

The measurements for the last month. One measurement is shown for each period of approx four hours (every 120th measurement, 168 values in all).

1 month

The measurements for the last 6 months. One measurement is shown for each period of approx one day (every 240th measurement, 180 values in all).

1 year

Measurements for the last 12 months. One measurement is shown for each two-day period (every 2880th measurement, 180 values in all).

Enable Power Monitoring

Specifies whether power monitoring is to be carried out.

Power Monitoring) is enabled by default as of Version 3.32 of the firmware.

This setting only applies to PRIMERGY servers that support consumption logging.

- Click *Apply* to activate your settings.
- Click *Delete History* to delete the displayed data.

Power History Chart

Power History Chart shows the power consumption of the managed server over time in the form of a graph (using the settings made under *Power History Options*). The difference between the actual power consumption and the power consumption displayed in the power history chart may amount to about 20%.

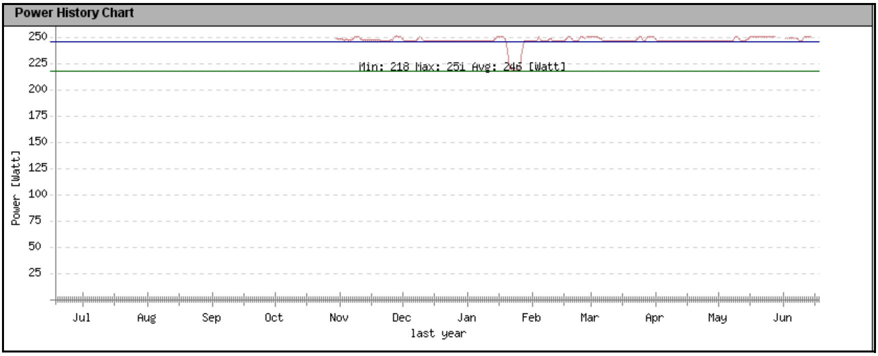


Figure 117: Power Consumption History - Power History Chart

7.9 Sensors - Check status of the sensors

The “Sensors” entry provides you with pages which allow you to check the statuses of sensors of the managed server:

– "Fans - Check fans" on page 212.

– "Temperature - Report the temperature of the server components" on page 215.

– "Voltages - Report voltage sensor information" on page 217.

– "Power Supply - Check power supply" on page 218.

– "Component Status - Check status of the server components" on page 220.

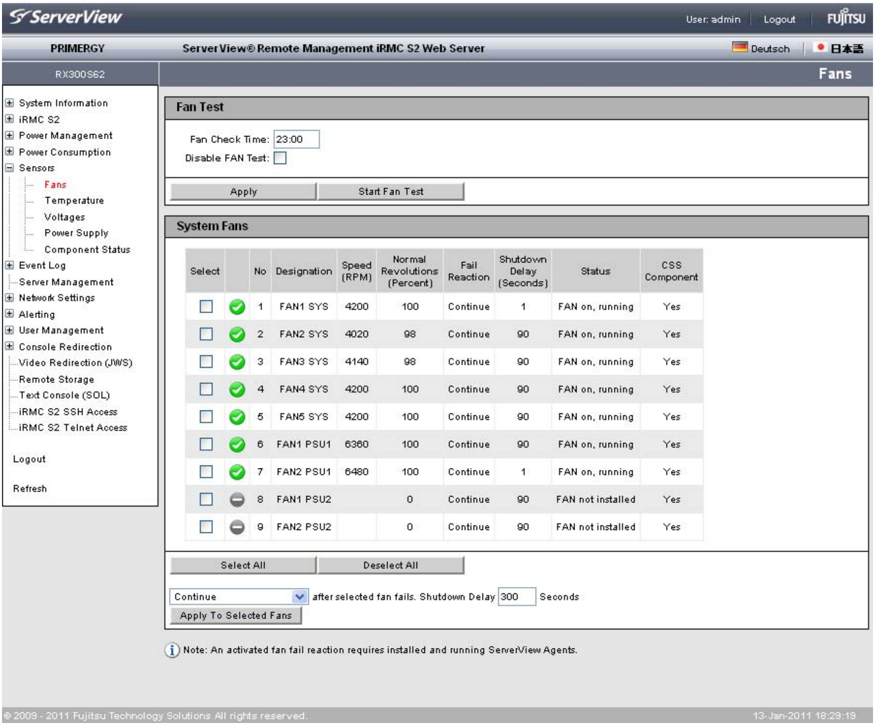
To facilitate checking the status, the sensor status is not only shown in the form of the current value, but also using a color code and a status icon:

Black (font color)/ ✓	The measured value is within the normal operational value range.
Orange (font color)/ ⚠	The measured value has exceeded the warning threshold. System operation is not yet jeopardized.
Red (font color)/ ✖	The measured value has exceeded the critical threshold. System operation may be jeopardized and there is a risk of loss of data integrity.

Table 6: Status of the sensors

7.9.1 Fans - Check fans

The *Fans* page provides information on fans and their status.



Fan Check Time: 23:00

Disable FAN Test: □

Select		No	Designation	Speed (RPM)	Normal Revolutions (Percent)	Fail Reaction	Shutdown Delay (Seconds)	Status	CSS Component
□	✓	1	FAN1 SYS	4200	100	Continue	1	FAN on, running	Yes
□	✓	2	FAN2 SYS	4020	98	Continue	90	FAN on, running	Yes
□	✓	3	FAN3 SYS	4140	98	Continue	90	FAN on, running	Yes
□	✓	4	FAN4 SYS	4200	100	Continue	90	FAN on, running	Yes
□	✓	5	FAN5 SYS	4200	100	Continue	90	FAN on, running	Yes
□	✓	6	FAN1 PSU1	6360	100	Continue	90	FAN on, running	Yes
□	✓	7	FAN2 PSU1	6480	100	Continue	1	FAN on, running	Yes
□	⊖	8	FAN1 PSU2		0	Continue	90	FAN not installed	Yes
□	⊖	9	FAN2 PSU2		0	Continue	90	FAN not installed	Yes

Continue after selected fan fails. Shutdown Delay 300 Seconds

Note: An activated fan fail reaction requires installed and running ServerView Agents.

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.

13-Jan-2011 18:29:19

Figure 118: Fans page

Fan Test - Test fans

The *Fan Test* group allows you to specify a time at which the fan test is started automatically or to start the fan test explicitly.

> **i** Instead of the formerly used full speed testing, most new systems now provide a modified fan test feature which performs the fan test with a speed near to the currently required speed. In this case, the fan test is no longer acoustically noticeable.

Fan Check Time

Enter the time at which the fan test is to be started automatically.

Disable Fan Test

Select this option to disable fan testing.

► Click *Apply* to activate your settings.

► Click *Start Fan Test* to start the fan test explicitly.

System Fans - Specify server behavior in the event that a fan fails

The *System Fans* group provides you with information on the status of the fans. You can use the options or buttons to select individual fans or all the fans and specify whether the server should be shut down after a specified number of seconds if this fan fails.

Select all

Selects all fans.

Deselect all

All selections are cancelled.

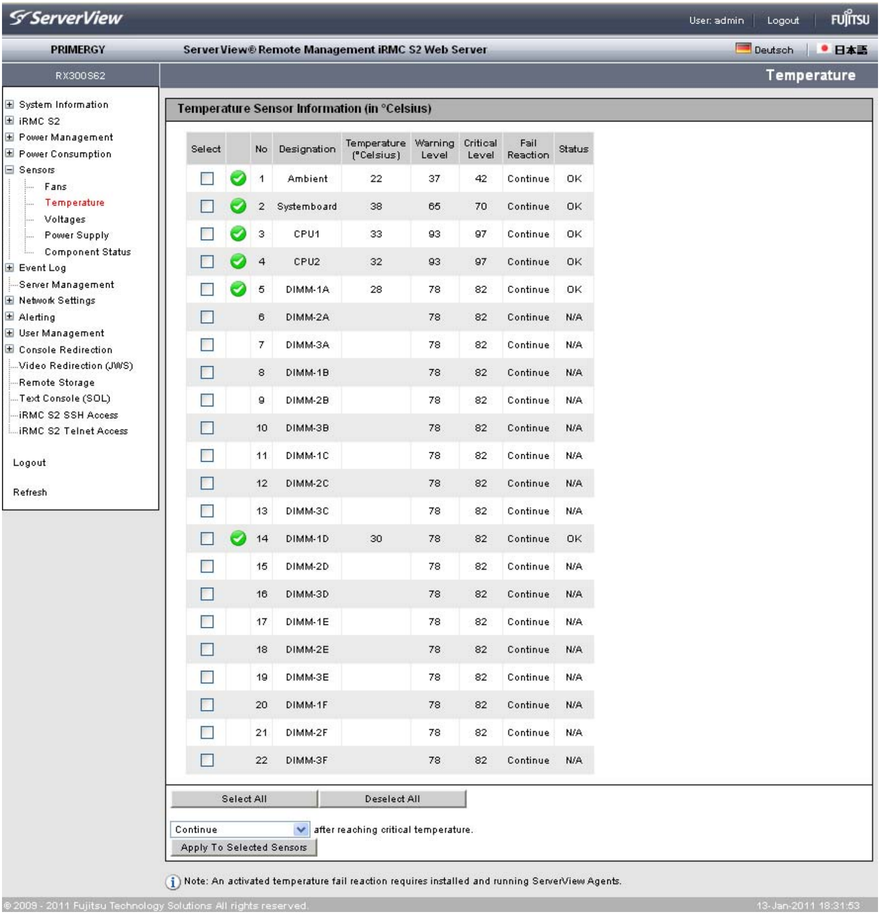
► Select the fans for which you wish to define the behavior in the event of a fault.

- ► Define the behavior in the event of a fault using the list at the bottom of the work area:
  - – Choose *continue* if the server is not to be shut down if the selected fans fail.
  - – Choose *shutdown-and-power-off* if the server is to be shut down and powered down if the selected fans fail. If you choose this option, you must also specify the time in seconds between failure of the fan and shutdown of the server (Shutdown Delay) in the field to the right of the list.

    i In the case of redundant fans, shutdown is only initiated if more than one fan is faulty and *shutdown-and-power-off* is also set for these fans.
- ► Click *Apply to the selected Fans* to activate your settings for the selected fans.

7.9.2 Temperature - Report the temperature of the server components

The *Temperature* page provides information on the status of the temperature sensors which measure the temperature at the server components, such as the CPU and the Memory Module and the ambient temperature.



Temperature Sensor Information (in °Celsius)

Select		No	Designation	Temperature (°Celsius)	Warning Level	Critical Level	Fail Reaction	Status
□	✓	1	Ambient	22	37	42	Continue	OK
□	✓	2	Systemboard	38	65	70	Continue	OK
□	✓	3	CPU1	33	93	97	Continue	OK
□	✓	4	CPU2	32	93	97	Continue	OK
□	✓	5	DIMM-1A	28	78	82	Continue	OK
□		6	DIMM-2A		78	82	Continue	N/A
□		7	DIMM-3A		78	82	Continue	N/A
□		8	DIMM-1B		78	82	Continue	N/A
□		9	DIMM-2B		78	82	Continue	N/A
□		10	DIMM-3B		78	82	Continue	N/A
□		11	DIMM-1C		78	82	Continue	N/A
□		12	DIMM-2C		78	82	Continue	N/A
□		13	DIMM-3C		78	82	Continue	N/A
□	✓	14	DIMM-1D	30	78	82	Continue	OK
□		15	DIMM-2D		78	82	Continue	N/A
□		16	DIMM-3D		78	82	Continue	N/A
□		17	DIMM-1E		78	82	Continue	N/A
□		18	DIMM-2E		78	82	Continue	N/A
□		19	DIMM-3E		78	82	Continue	N/A
□		20	DIMM-1F		78	82	Continue	N/A
□		21	DIMM-2F		78	82	Continue	N/A
□		22	DIMM-3F		78	82	Continue	N/A

Continue after reaching critical temperature.

Note: An activated temperature fail reaction requires installed and running ServerView Agents.

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.

13-Jan-2011 18:31:53

Figure 119: Temperature page

You can use the options or buttons to select individual temperature sensors or all the temperature sensors and specify whether the server is to be shut down if the critical temperature is reached at the selected sensors.

Select all

Selects all temperature sensors.

Deselect all

All selections are cancelled.

► Select the sensors for which you wish to define the behavior in the event that the critical temperature is reached.

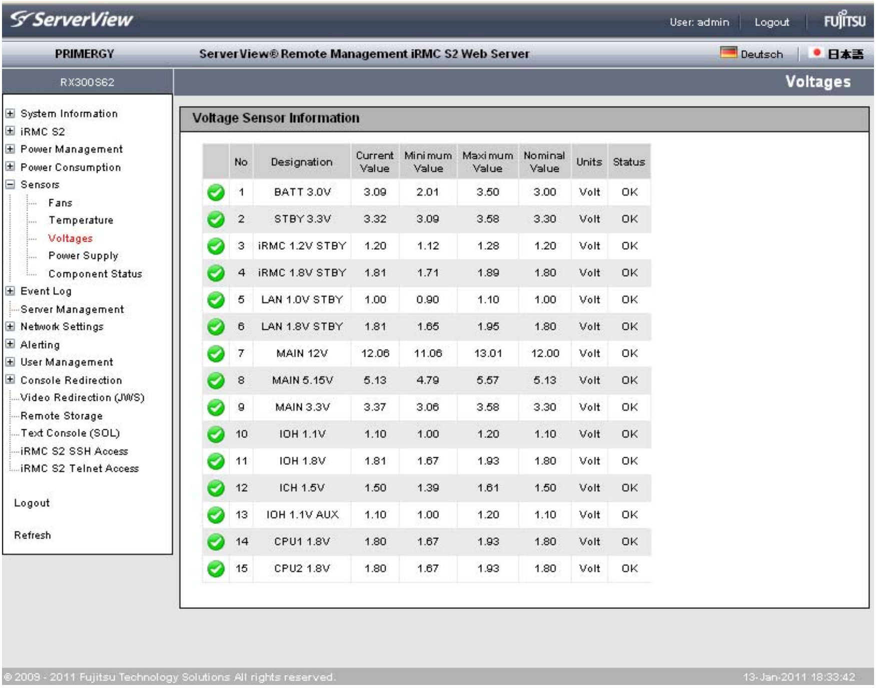
► Define the behavior in the event that the critical temperature is reached using the list at the bottom of the work area:

- Choose *continue* if the server is not to be shut down if the critical temperature is reached at the selected sensors.
- Choose *shutdown-and-power-off* if the server is to be shut down and powered down if the critical temperature is reached at the selected sensors.

► Click *Apply to the selected Sensors* to activate your settings for the selected temperature sensors.

7.9.3 Voltages - Report voltage sensor information

The *Voltages* page provides information on the status of voltage sensors assigned to the server components.



Voltage Sensor Information

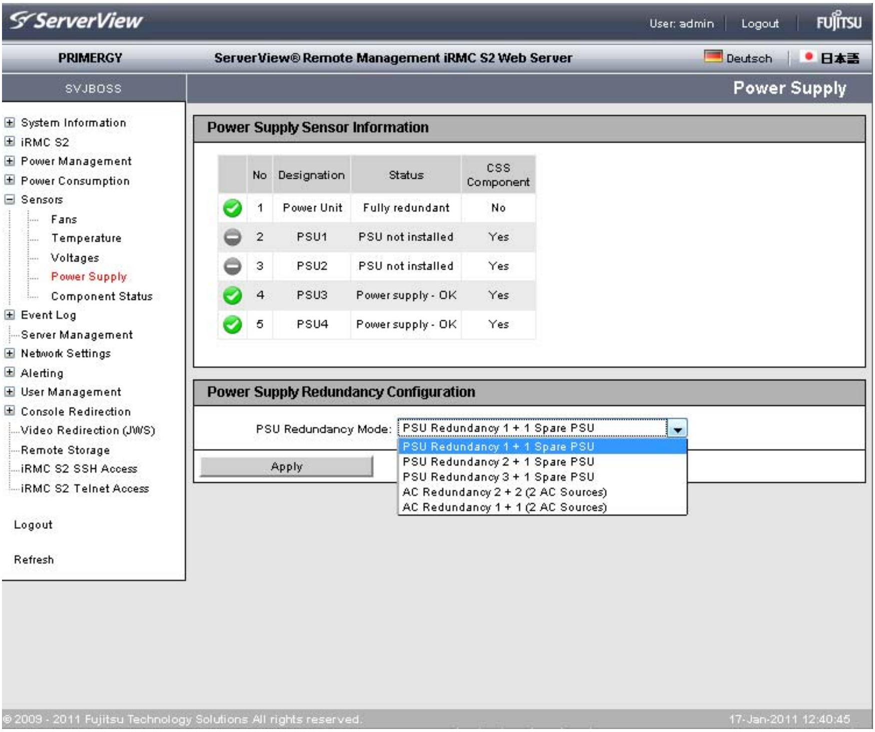
	No	Designation	Current Value	Minimum Value	Maximum Value	Nominal Value	Units	Status
✓	1	BATT 3.0V	3.09	2.01	3.50	3.00	Volt	OK
✓	2	STBY 3.3V	3.32	3.09	3.58	3.30	Volt	OK
✓	3	iRMC 1.2V STBY	1.20	1.12	1.28	1.20	Volt	OK
✓	4	iRMC 1.8V STBY	1.81	1.71	1.89	1.80	Volt	OK
✓	5	LAN 1.0V STBY	1.00	0.90	1.10	1.00	Volt	OK
✓	6	LAN 1.8V STBY	1.81	1.65	1.95	1.80	Volt	OK
✓	7	MAIN 12V	12.06	11.06	13.01	12.00	Volt	OK
✓	8	MAIN 5.15V	5.13	4.79	5.57	5.13	Volt	OK
✓	9	MAIN 3.3V	3.37	3.06	3.58	3.30	Volt	OK
✓	10	IOH 1.1V	1.10	1.00	1.20	1.10	Volt	OK
✓	11	IOH 1.8V	1.81	1.67	1.93	1.80	Volt	OK
✓	12	ICH 1.5V	1.50	1.39	1.61	1.50	Volt	OK
✓	13	IOH 1.1V AUX	1.10	1.00	1.20	1.10	Volt	OK
✓	14	CPU1 1.8V	1.80	1.67	1.93	1.80	Volt	OK
✓	15	CPU2 1.8V	1.80	1.67	1.93	1.80	Volt	OK

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.   13-Jan-2011 18:33:42

Figure 120: Voltages page

7.9.4 Power Supply - Check power supply

The *Power Supply* page provides information on the power supplied from the power supply units. For some server types, the *Power Supply* page also allows you to configure power supply redundancy settings.



Power Supply Sensor Information

	No	Designation	Status	CSS Component
✓	1	Power Unit	Fully redundant	No
⊖	2	PSU1	PSU not installed	Yes
⊖	3	PSU2	PSU not installed	Yes
✓	4	PSU3	Power supply - OK	Yes
✓	5	PSU4	Power supply - OK	Yes

Power Supply Redundancy Configuration

PSU Redundancy Mode: PSU Redundancy 1 + 1 Spare PSU

Figure 121: Power Supply page

Power Supply Redundancy Configuration

i This functionality is not available with all servers.

The *Power Supply Redundancy Configuration* group allows you to set the redundancy mode for the managed server. It depends on the servers capabilities which options are actually available.

PSU Redundancy 1 + 1 Spare PSU
System operation is guaranteed for 1 PSU fail in the case of 2 PSUs in total.

PSU Redundancy 2+ 1 Spare PSU
System operation is guaranteed for 1 PSU fail in the case of 3 PSUs in total.

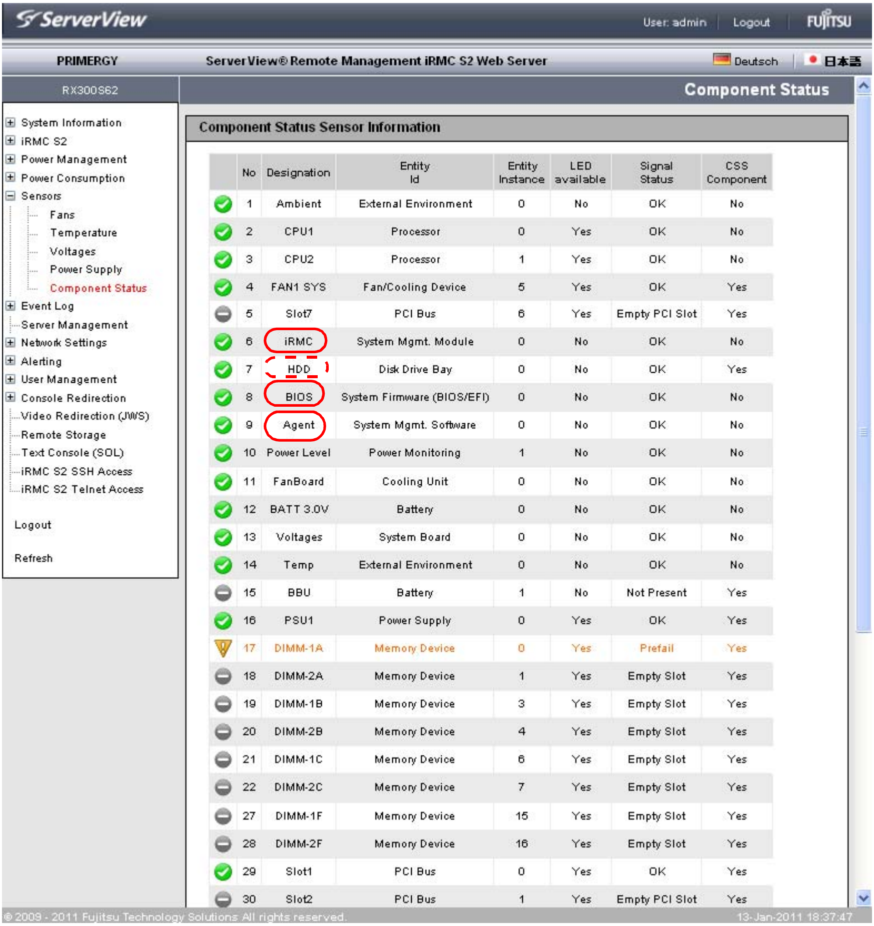
PSU Redundancy 3+ 1 Spare PSU
System operation is guaranteed for 1 PSU fail in the case of 4 PSUs in total.

AC Redundancy 2 + 2 (2 AC sources)
2 of the 4 PSUs are each connected to a separate AC source. This ensures that the system can continue operation even if a power line or a single PSU fails.

AC Redundancy 1 + 1 (2 AC sources)
Each PSU (of 2 PSUs in total) is connected to a separate AC source. This ensures that the system can continue operation even if a power line or a single PSU fails.

7.9.5 Component Status - Check status of the server components

The *Component Status* page provides information on the status of the server components. The *CSS Component* column indicates for each of the components whether the CSS (**C**ustomer **S**elf **S**ervice) functionality is supported.



Component Status Sensor Information

	No	Designation	Entity Id	Entity Instance	LED available	Signal Status	CSS Component
✓	1	Ambient	External Environment	0	No	OK	No
✓	2	CPU1	Processor	0	Yes	OK	No
✓	3	CPU2	Processor	1	Yes	OK	No
✓	4	FAN1 SYS	Fan/Cooling Device	5	Yes	OK	Yes
⊖	5	Slot7	PCI Bus	6	Yes	Empty PCI Slot	Yes
✓	6	iRMC	System Mgmt. Module	0	No	OK	No
✓	7	HDD	Disk Drive Bay	0	No	OK	Yes
✓	8	BIOS	System Firmware (BIOS/EFI)	0	No	OK	No
✓	9	Agent	System Mgmt. Software	0	No	OK	No
✓	10	Power Level	Power Monitoring	1	No	OK	No
✓	11	FanBoard	Cooling Unit	0	No	OK	No
✓	12	BATT 3.0V	Battery	0	No	OK	No
✓	13	Voltages	System Board	0	No	OK	No
✓	14	Temp	External Environment	0	No	OK	No
⊖	15	BBU	Battery	1	No	Not Present	Yes
✓	16	PSU1	Power Supply	0	Yes	OK	Yes
⚠	17	DIMM-1A	Memory Device	0	Yes	Prefail	Yes
⊖	18	DIMM-2A	Memory Device	1	Yes	Empty Slot	Yes
⊖	19	DIMM-1B	Memory Device	3	Yes	Empty Slot	Yes
⊖	20	DIMM-2B	Memory Device	4	Yes	Empty Slot	Yes
⊖	21	DIMM-1C	Memory Device	6	Yes	Empty Slot	Yes
⊖	22	DIMM-2C	Memory Device	7	Yes	Empty Slot	Yes
⊖	27	DIMM-1F	Memory Device	15	Yes	Empty Slot	Yes
⊖	28	DIMM-2F	Memory Device	16	Yes	Empty Slot	Yes
✓	29	Slot1	PCI Bus	0	Yes	OK	Yes
⊖	30	Slot2	PCI Bus	1	Yes	Empty PCI Slot	Yes

Figure 122: Component Status page

Entries with Designation "iRMC", "Agent", "BIOS", or "VIOM"

Entries with the *Designation* "iRMC", "Agent", "BIOS", or "VIOM" indicate that the iRMC S2/S3, the agent, the BIOS, or VIOM has detected an error. It does not mean that the iRMC S2/S3, the agent, the BIOS, or VIOM itself is defective.

Entries with Designation "HDD" and "HDD<n>, agentless HDD monitoring ("out-of-band" HDD monitoring)

Entries with the *Designation* "HDD" or "HDD<n>" (with n = 1, 2, ...) indicate the statuses of Hard Disk Drives (HDD):

– The entry with *Designation* "HDD" indicates the overall HDD status of the server by summarizing the statuses of the individual HDDs.

  The overall HDD status of the server is read and reported to the iRMC S2/S3 by the ServerView agents and the ServerView RAID Manager.

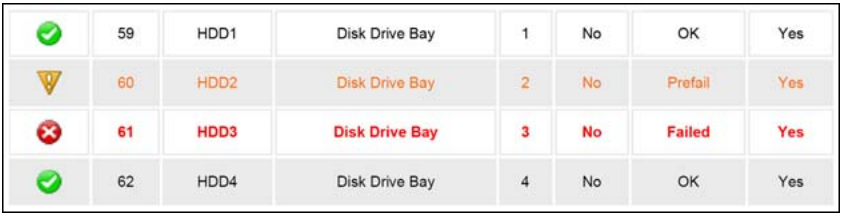
– An entry with *Designation* "HDD<n>" (where n = 1, 2, ...) indicates the status of an individual HDD.

  Please note:

  – This feature is only supported by the iRMC S3.

  – This feature only supported if the managed PRIMERGY server supports the "agentless HDD monitoring" function (also known as "out-of-band HDD monitoring").

  If these requirements are met, the HDD<n> status of each individual HDD is reported directly to the iRMC S3, i.e. without using the ServerView agents.



✓	59	HDD1	Disk Drive Bay	1	No	OK	Yes
⚠	60	HDD2	Disk Drive Bay	2	No	Prefail	Yes
✗	61	HDD3	Disk Drive Bay	3	No	Failed	Yes
✓	62	HDD4	Disk Drive Bay	4	No	OK	Yes

Figure 123: Status display for individual HDDs

i The precise entries displayed in the *Component Status Sensor Information* table, therefore, depend on the server state and whether the server supports "agentless HDD monitoring":

- The entry with *Designation* "HDD" only shows a status in the *Signal Status* column if the ServerView agents and the ServerView RAID Manager are installed and running on the managed server. Otherwise, "N/A" (not available) is displayed in the *Signal Status* column instead.
- The entries with *Designation* "HDD<n> (with n = 1, 2, ...)" are only displayed if the managed server supports "agentless HDD monitoring".

7.10 System Event Log and Internal Event Log

The *Event Log* entry in the navigation area contains the links to the pages for viewing and configuring the IPMI event log (system event log, SEL) and the iRMC S2/S3 internal event log:

– "System Event Log Content - Show information on the SEL and the SEL entries" on page 224.

  The internal event log contains entries providing information on audit events (logon events, AVR connection events, etc.) and additional information (e.g. IPv6 related information and LDAP user names).

– "Internal Event Log Content - Show information on the internal eventlog and the associated entries" on page 227.

  The IPMI SEL contains entries providing information on events like operating system boots / shutdowns, fan failures, and iRMC S2/S3 firmware flashes.

– "Event Log Configuration - Configure IPMI SEL and internal event log" on page 230.

Colored icons are assigned to the various event / error categories to improve clarity:

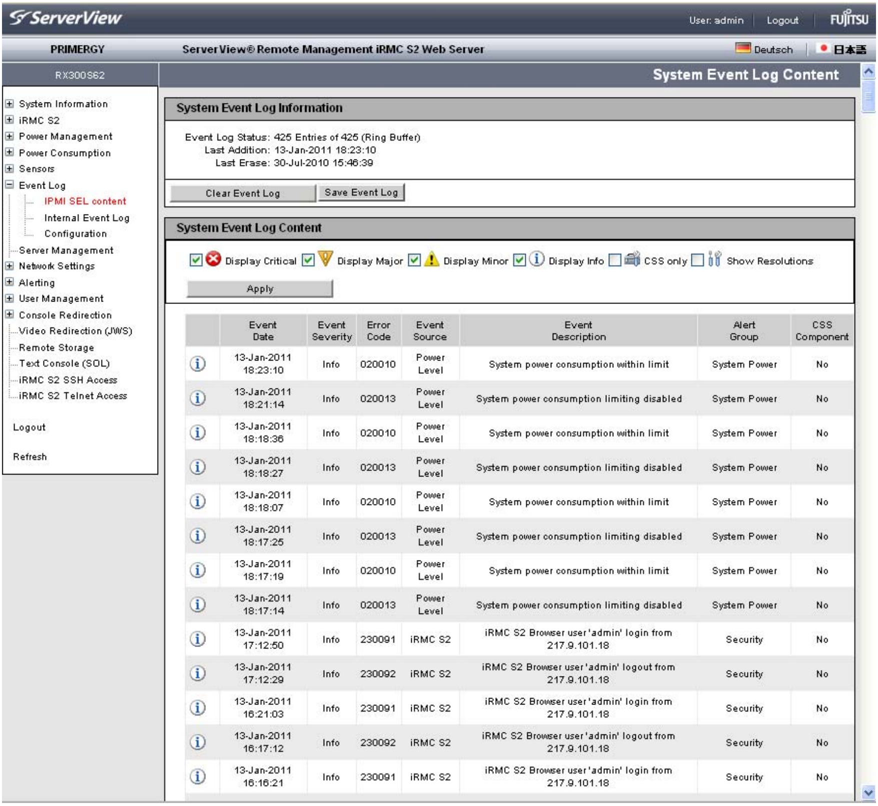
✖	Critical
❗	Major
⚠	Minor
ℹ	Informational
🧰	Customer Self Service (CSS) event

Table 7: System event log / internal event log content - error categories

7.10.1 System Event Log Content - Show information on the SEL and the SEL entries

The *System Event Log Content* page provides information on the IPMI SEL and displays the SEL entries. The IPMI SEL contains entries providing information on events like operating system boots / shutdowns, fan failures, and iRMC S2/S3 firmware flashes.

The *CSS Event* column indicates for each of the events whether the event was triggered by a CSS (**C**ustomer **S**elf **S**ervice) component.



Event Log Status: 425 Entries of 425 (Ring Buffer)
Last Addition: 13-Jan-2011 18:23:10
Last Erase: 30-Jul-2010 15:46:39

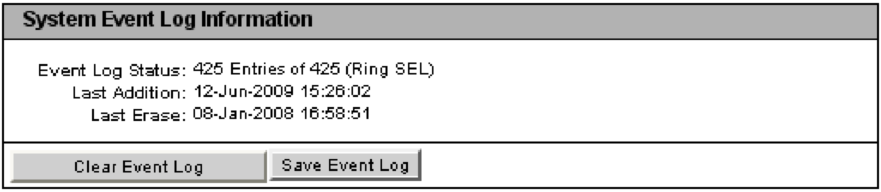
☑ Display Critical ☑ Display Major ☑ Display Minor ☑ Display Info □ CSS only □ Show Resolutions

	Event Date	Event Severity	Error Code	Event Source	Event Description	Alert Group	CSS Component
ⓘ	13-Jan-2011 18:23:10	Info	020010	Power Level	System power consumption within limit	System Power	No
ⓘ	13-Jan-2011 18:21:14	Info	020013	Power Level	System power consumption limiting disabled	System Power	No
ⓘ	13-Jan-2011 18:18:36	Info	020010	Power Level	System power consumption within limit	System Power	No
ⓘ	13-Jan-2011 18:18:27	Info	020013	Power Level	System power consumption limiting disabled	System Power	No
ⓘ	13-Jan-2011 18:18:07	Info	020010	Power Level	System power consumption within limit	System Power	No
ⓘ	13-Jan-2011 18:17:25	Info	020013	Power Level	System power consumption limiting disabled	System Power	No
ⓘ	13-Jan-2011 18:17:19	Info	020010	Power Level	System power consumption within limit	System Power	No
ⓘ	13-Jan-2011 18:17:14	Info	020013	Power Level	System power consumption limiting disabled	System Power	No
ⓘ	13-Jan-2011 17:12:50	Info	230091	iRMC S2	iRMC S2 Browser user 'admin' login from 217.9.101.18	Security	No
ⓘ	13-Jan-2011 17:12:29	Info	230092	iRMC S2	iRMC S2 Browser user 'admin' logout from 217.9.101.18	Security	No
ⓘ	13-Jan-2011 16:21:03	Info	230091	iRMC S2	iRMC S2 Browser user 'admin' login from 217.9.101.18	Security	No
ⓘ	13-Jan-2011 16:17:12	Info	230092	iRMC S2	iRMC S2 Browser user 'admin' logout from 217.9.101.18	Security	No
ⓘ	13-Jan-2011 16:16:21	Info	230091	iRMC S2	iRMC S2 Browser user 'admin' login from 217.9.101.18	Security	No

Figure 124: System Event Log Content page

System Event Log Information

The *System Event Log Information* group informs you of the number of entries in the IPMI SEL. It also indicates the time when the last entries were added or deleted.



System Event Log Information

Event Log Status: 425 Entries of 425 (Ring SEL)
Last Addition: 12-Jun-2009 15:26:02
Last Erase: 08-Jan-2008 16:58:51

Figure 125: System Event Log Content page, System Event Log Information

Clear Event Log

Click *Clear Event Log* to clear all the entries in the IPMI SEL.

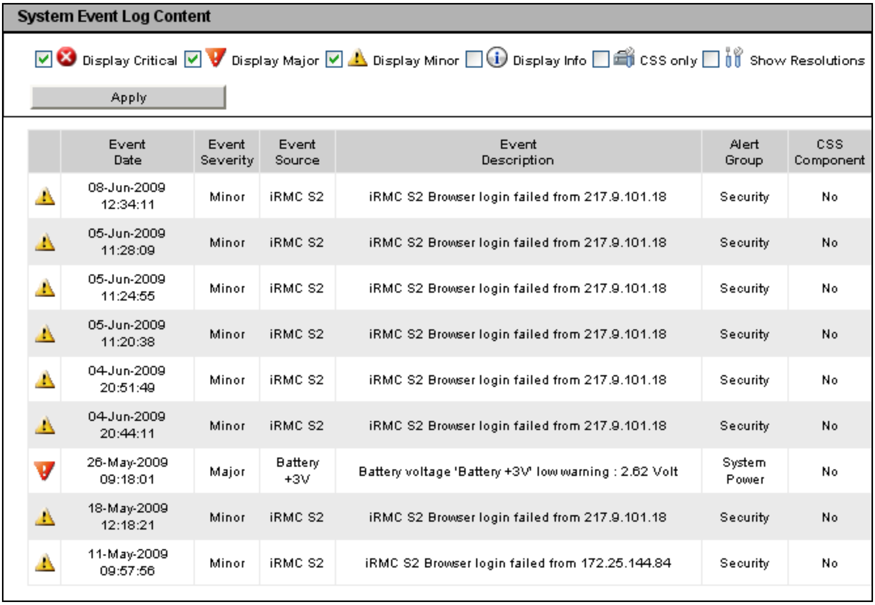
Save Event Log

After you have clicked *Save Event Log*, the iRMC S2/S3 allows you to download the file *iRMC S2/S3_EventLog.sel*, which contains the IPMI SEL entries.

System Event Log Content

The *System Event Log Content* group displays the SEL entries filtered by severity class.

> You can modify the filter criteria for the duration of the current session in the *System Event Log Content* group. However, the settings you make here are only valid until the next logout. After that, the default settings apply again.



System Event Log Content

☑ Display Critical ☑ Display Major ☑ Display Minor □ Display Info □ CSS only □ Show Resolutions

Apply

	Event Date	Event Severity	Event Source	Event Description	Alert Group	CSS Component
⚠	08-Jun-2009 12:34:11	Minor	iRMC S2	iRMC S2 Browser login failed from 217.9.101.18	Security	No
⚠	05-Jun-2009 11:28:09	Minor	iRMC S2	iRMC S2 Browser login failed from 217.9.101.18	Security	No
⚠	05-Jun-2009 11:24:55	Minor	iRMC S2	iRMC S2 Browser login failed from 217.9.101.18	Security	No
⚠	05-Jun-2009 11:20:38	Minor	iRMC S2	iRMC S2 Browser login failed from 217.9.101.18	Security	No
⚠	04-Jun-2009 20:51:49	Minor	iRMC S2	iRMC S2 Browser login failed from 217.9.101.18	Security	No
⚠	04-Jun-2009 20:44:11	Minor	iRMC S2	iRMC S2 Browser login failed from 217.9.101.18	Security	No
▼	26-May-2009 09:18:01	Major	Battery +3V	Battery voltage 'Battery +3V' low warning : 2.62 Volt	System Power	No
⚠	18-May-2009 12:18:21	Minor	iRMC S2	iRMC S2 Browser login failed from 217.9.101.18	Security	No
⚠	11-May-2009 09:57:56	Minor	iRMC S2	iRMC S2 Browser login failed from 172.25.144.84	Security	No

Figure 126: System Event Log Content page, System Event Log Content

Display Critical, *Display Major*, *Display Minor*, *Display Info*, *CSS only*

If you wish, you can choose one or more severity levels other than the default values here.

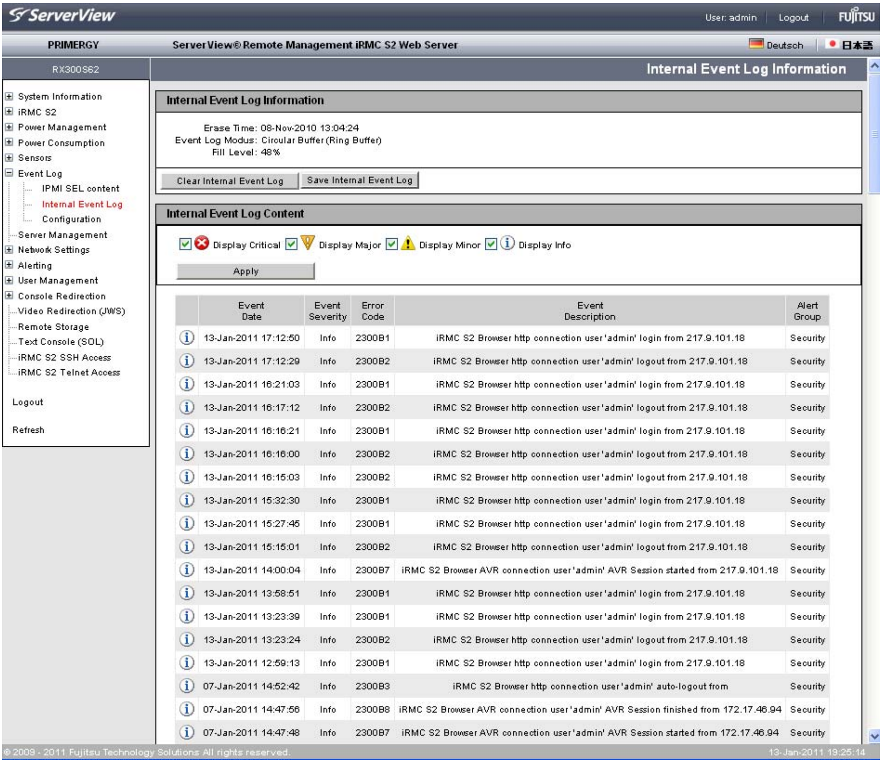
Show Resolutions

If you choose this option, a proposal for solution will be displayed for each SEL entry of severity level *Critical* or *Major*.

► Click *Apply* to activate your settings for the duration of the current session.

7.10.2 Internal Event Log Content - Show information on the internal eventlog and the associated entries

The *Internal Event Log Content* page provides information on the internal eventlog and displays the associated entries. The internal event log comprises audit events (logon events, AVR connection events, etc.) and additional information (e.g. IPv6 related information and LDAP user names).



Internal Event Log Information

Erase Time: 08-Nov-2010 13:04:24
Event Log Modus: Circular Buffer (Ring Buffer)
Fill Level: 48%

Internal Event Log Content

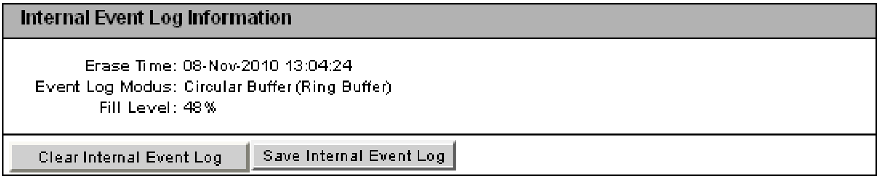
☑ Display Critical ☑ Display Major ☑ Display Minor ☑ Display Info

	Event Date	Event Severity	Error Code	Event Description	Alert Group
ⓘ	13-Jan-2011 17:12:50	Info	2300B1	iRMC S2 Browser http connection user 'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 17:12:29	Info	2300B2	iRMC S2 Browser http connection user 'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 16:21:03	Info	2300B1	iRMC S2 Browser http connection user 'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 16:17:12	Info	2300B2	iRMC S2 Browser http connection user 'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 16:16:21	Info	2300B1	iRMC S2 Browser http connection user 'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 16:16:00	Info	2300B2	iRMC S2 Browser http connection user 'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 16:15:03	Info	2300B2	iRMC S2 Browser http connection user 'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 15:32:30	Info	2300B1	iRMC S2 Browser http connection user 'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 15:27:45	Info	2300B1	iRMC S2 Browser http connection user 'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 15:15:01	Info	2300B2	iRMC S2 Browser http connection user 'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 14:00:04	Info	2300B7	iRMC S2 Browser AVR connection user 'admin' AVR Session started from 217.9.101.18	Security
ⓘ	13-Jan-2011 13:58:51	Info	2300B1	iRMC S2 Browser http connection user 'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 13:23:39	Info	2300B1	iRMC S2 Browser http connection user 'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 13:23:24	Info	2300B2	iRMC S2 Browser http connection user 'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 12:59:13	Info	2300B1	iRMC S2 Browser http connection user 'admin' login from 217.9.101.18	Security
ⓘ	07-Jan-2011 14:52:42	Info	2300B3	iRMC S2 Browser http connection user 'admin' auto-logout from	Security
ⓘ	07-Jan-2011 14:47:56	Info	2300B8	iRMC S2 Browser AVR connection user 'admin' AVR Session finished from 172.17.46.94	Security
ⓘ	07-Jan-2011 14:47:48	Info	2300B7	iRMC S2 Browser AVR connection user 'admin' AVR Session started from 172.17.46.94	Security

Figure 127: InternalEvent Log Content page

Internal Event Log Information

The *Internal Event Log Information* group informs you of the number of entries in the internal event log. It also indicates the time when the last entries were added or deleted.



Internal Event Log Information

Erase Time: 08-Nov-2010 13:04:24
Event Log Modus: Circular Buffer (Ring Buffer)
Fill Level: 48%

Figure 128: System Event Log Content page, System Event Log Information

Clear Internal Event Log

Click *Clear Internal Event Log* to clear all the entries in the internal event log.

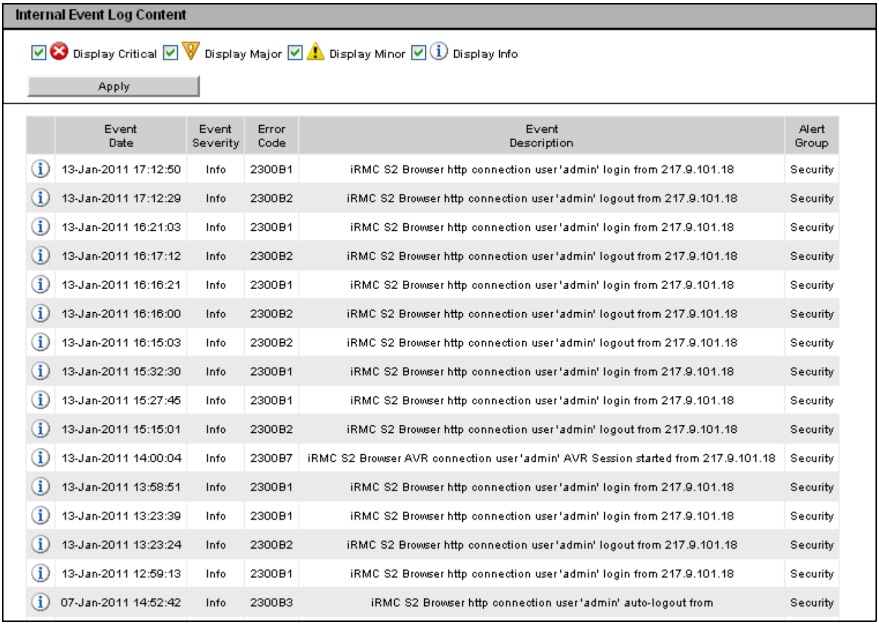
Save Internal Event Log

After you have clicked *Save Internal Event Log*, the iRMC S2/S3 allows you to download the file *iRMC S2_InternalEventLog.sel* / the file *iRMC S3_InternalEventLog.sel*, which contains the entries of the internal event log.

Internal Event Log Content

The *Internal Event Log Content* group displays the internal eventlog entries filtered by severity class.

> **i** You can modify the filter criteria for the duration of the current session in the *Internal Event Log Content* group. However, the settings you make here are only valid until the next logout. After that, the default settings apply again.



Internal Event Log Content

☑ Display Critical ☑ Display Major ☑ Display Minor ☑ Display Info

Apply

	Event Date	Event Severity	Error Code	Event Description	Alert Group
ⓘ	13-Jan-2011 17:12:50	Info	2300B1	iRMC S2 Browser http connection user'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 17:12:29	Info	2300B2	iRMC S2 Browser http connection user'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 16:21:03	Info	2300B1	iRMC S2 Browser http connection user'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 16:17:12	Info	2300B2	iRMC S2 Browser http connection user'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 16:16:21	Info	2300B1	iRMC S2 Browser http connection user'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 16:16:00	Info	2300B2	iRMC S2 Browser http connection user'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 16:15:03	Info	2300B2	iRMC S2 Browser http connection user'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 15:32:30	Info	2300B1	iRMC S2 Browser http connection user'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 15:27:45	Info	2300B1	iRMC S2 Browser http connection user'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 15:15:01	Info	2300B2	iRMC S2 Browser http connection user'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 14:00:04	Info	2300B7	iRMC S2 Browser AVR connection user'admin' AVR Session started from 217.9.101.18	Security
ⓘ	13-Jan-2011 13:58:51	Info	2300B1	iRMC S2 Browser http connection user'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 13:23:39	Info	2300B1	iRMC S2 Browser http connection user'admin' login from 217.9.101.18	Security
ⓘ	13-Jan-2011 13:23:24	Info	2300B2	iRMC S2 Browser http connection user'admin' logout from 217.9.101.18	Security
ⓘ	13-Jan-2011 12:59:13	Info	2300B1	iRMC S2 Browser http connection user'admin' login from 217.9.101.18	Security
ⓘ	07-Jan-2011 14:52:42	Info	2300B3	iRMC S2 Browser http connection user'admin' auto-logout from	Security

Figure 129: System Event Log Content page, System Event Log Content

Display Critical, *Display Major*, *Display Minor*, *Display Info*

If you wish, you can choose one or more severity levels other than the default values here.

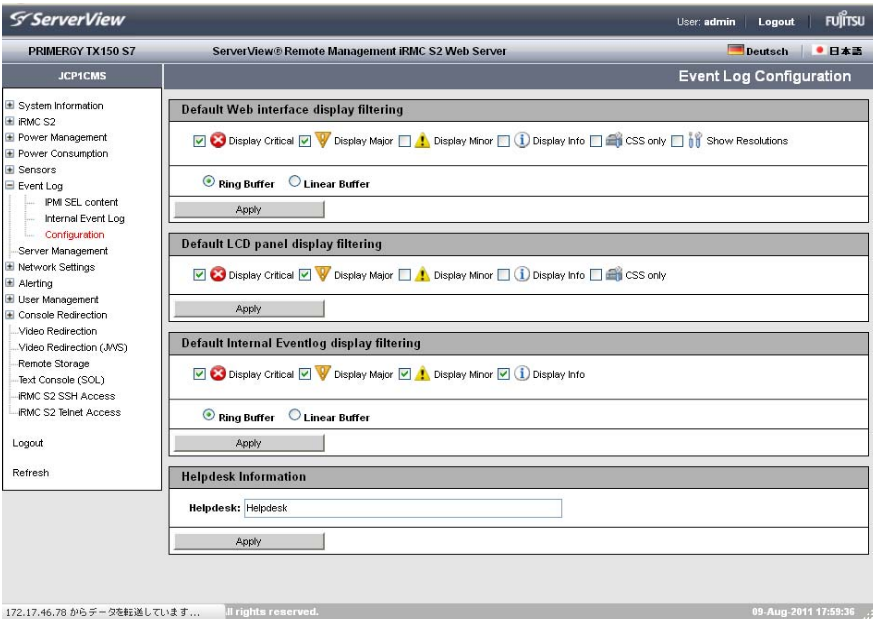
► Click *Apply* to activate your settings for the duration of the current session.

7.10.3 Event Log Configuration - Configure IPMI SEL and internal event log

On the *Event Log Configuration* page, you can configure the IPMI system event log (SEL) and the internal eventlog.

You can configure for each of the event logs

- the entries which are displayed by default on the *System Event Log Content* page (see page 224) and on the *Internal Event Log Content* page (see page 227), respectively.
- whether IPMI SEL and internal eventlog are organized as a ring buffer or a linear buffer.



Event Log Configuration

Default Web interface display filtering

☑ Display Critical ☑ Display Major □ Display Minor □ Display Info □ CSS only □ Show Resolutions

● Ring Buffer ○ Linear Buffer

Apply

Default LCD panel display filtering

☑ Display Critical ☑ Display Major □ Display Minor □ Display Info □ CSS only

Apply

Default Internal Eventlog display filtering

☑ Display Critical ☑ Display Major ☑ Display Minor ☑ Display Info

● Ring Buffer ○ Linear Buffer

Apply

Helpdesk Information

Helpdesk: Helpdesk

Apply

172.17.46.78 からデータを転送しています... ll rights reserved. 09-Aug-2011 17:59:36

Figure 130: Event Log Configuration page

IPMI Event Log Configuration

Default LCD panel display filtering

> If a ServerView Local Service Display module is fitted in the managed PRIMERGY server, you can also select the error severities for displaying the SEL on the ServerView Local Service Display. (This selection is independent of the selection you have made for the SEL entries displayed on the *System Event Log Content* page.)

Display Critical, *Display Major*, *Display Minor*, *Display Info*, *CSS only*

Here you select one or more severity levels for which event log entries should be displayed by default on the on the ServerView Local Service Display.

Default Web interface display filtering

Display Critical, *Display Major*, *Display Minor*, *Display Info*, *CSS only*

Here you select one or more severity levels for which event log entries should be displayed by default on the on the *System Event Log Content* page (see page 224).

Show Resolutions

If you choose this option, the cause of the entry and a proposal for resolution will be displayed for each SEL entry of severity level *Critical*, *Major*, or *Minor*.

Ring Buffer

The event log is organized as a ring buffer.

Linear Buffer

The event log is organized as a linear buffer.

> When the linear event log has been completely filled, it is not possible to add any further entries.

- Click *Apply* to activate your settings.

Internal Event Log Configuration

Display Critical, *Display Major*, *Display Minor*, *Display Info*

Here you select one or more severity levels for which event log entries should be displayed by default on the on the *Internal Event Log Content* page (see page 227).

Ring Buffer

The event log is organized as a ring buffer.

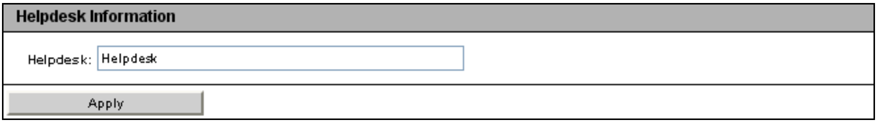
Linear Buffer

The event log is organized as a linear buffer.

i When the linear event log has been completely filled, it is not possible to add any further entries.

- Click *Apply* to activate your settings.

Helpdesk Information



Helpdesk Information

Helpdesk: Helpdesk

Figure 131: Helpdesk Information

Help desk

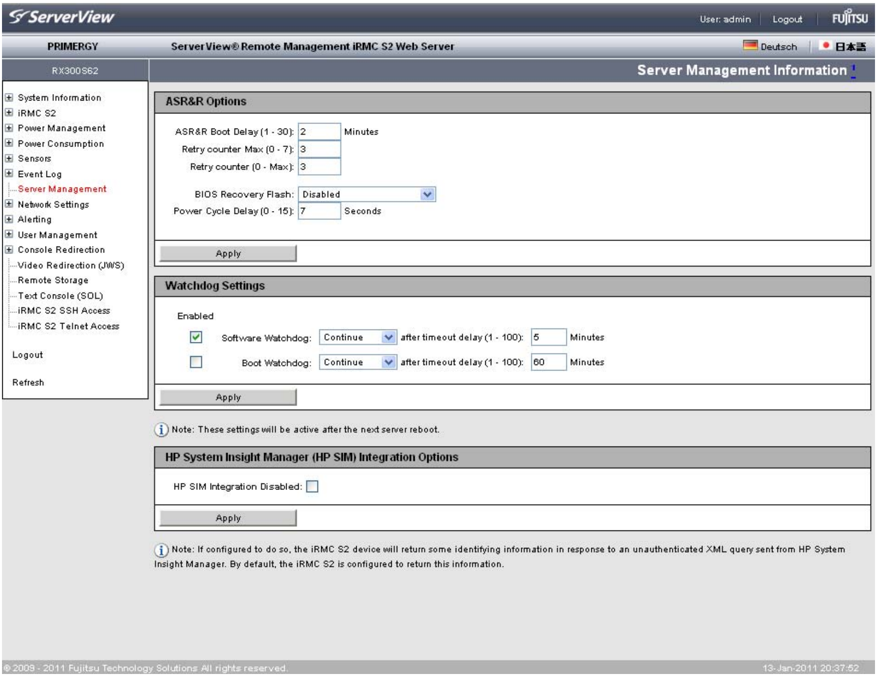
String used to display the Help Desk

- Click *Apply* to activate your settings.

7.11 Server Management Information - Configuring the server settings

The *Server Management Information* page allows you to configure the following settings on the server:

- ASR&R (automatic server reconfiguration and restart) settings for the server (see page 234)
- Watchdog settings (see page 235)
- HP System Insight Manager (HP SIM) integration (see page 237)



ASR&R Options

ASR&R Boot Delay (1 - 30): 2 Minutes
Retry counter Max (0 - 7): 3
Retry counter (0 - Max): 3
BIOS Recovery Flash: Disabled
Power Cycle Delay (0 - 15): 7 Seconds

Watchdog Settings

Enabled
☑ Software Watchdog: Continue after timeout delay (1 - 100): 5 Minutes
□ Boot Watchdog: Continue after timeout delay (1 - 100): 60 Minutes

Note: These settings will be active after the next server reboot.

HP System Insight Manager (HP SIM) Integration Options

HP SIM Integration Disabled: □

Note: If configured to do so, the iRMC S2 device will return some identifying information in response to an unauthenticated XML query sent from HP System Insight Manager. By default, the iRMC S2 is configured to return this information.

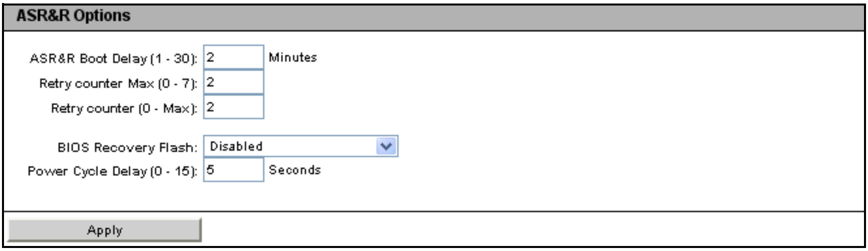
© 2009 - 2011 Fujitsu Technology Solutions All rights reserved. 13-Jan-2011 20:37:52

Figure 132: Server Management Information page

ASR&R Options - Configure ASR&R settings

The *ASR&R Options* group allows you to configure the ASR&R (automatic server reconfiguration and restart) settings for the server.

i The settings made on the *ASR&R Options* group become active the next time the managed server is started.



ASR&R Options

ASR&R Boot Delay (1 - 30): 2 Minutes
Retry counter Max (0 - 7): 2
Retry counter (0 - Max): 2
BIOS Recovery Flash: Disabled
Power Cycle Delay (0 - 15): 5 Seconds

Figure 133: Server Management Information page, ASR&R Options

Retry counter Max (0 - 7)

Maximum number of restart attempts that should be permitted for the server after a critical error (up to 7).

Retry counter (0 - Max)

Number of restart attempts that a server should attempt after a critical error (maximum value is the value set under *Retry counter Max*).

BIOS recovery flash bit

Enables/disables the BIOS recovery flash bit:

– *Enabled*
  The next time the system is booted, the BIOS is automatically flashed.

– *Disabled*
  The next time the system is booted, the BIOS is not automatically flashed.

i The *Enabled* setting is of value if the operating system no longer boots after the firmware has been updated. A BIOS recovery flash is then performed automatically the next time the system is booted from the DOS floppy (or a DOS floppy image).

After a BIOS recovery flash has been performed successfully, reset the BIOS Recovery Flash bit to *disabled*.

Power Cycle Delay (0 - 15)

Time (in seconds) between powering down and powering up during a power cycle.

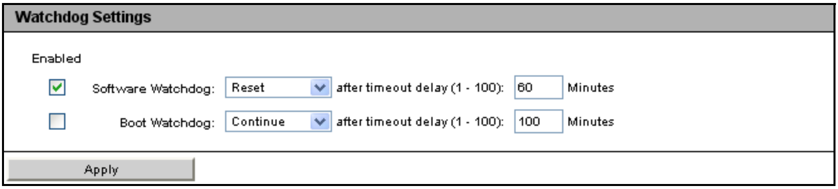
► Click *Apply* to save your settings.

The configured settings are saved and the actions which have been configured are performed in the appropriate circumstances.

Watchdog Settings - Configure software watchdog and boot watchdog

The *Watchdog Settings* group allows you configure the software watchdog and the boot watchdog.

i The settings made on the *ASR&R Options* group become active the next time the managed server is started.



Watchdog Settings

Enabled

☑ Software Watchdog: Reset after timeout delay (1 - 100): 60 Minutes

☐ Boot Watchdog: Continue after timeout delay (1 - 100): 100 Minutes

Figure 134: Server Management Information page, Watchdog Options

The **software** watchdog

monitors the activities of system using the ServerView agents. The software watchdog is activated when the ServerView agents and the operating system have been completely initialized.
The ServerView agents contact the iRMC S2/S3 at defined intervals. If no more messages are received from a ServerView agent, it is assumed that the system is no longer functioning correctly.
You can specify an action to be performed if this happens.

The **boot watchdog** monitors the phase between startup of the system and the time at which the ServerView agents become available.
If the ServerView agents do not establish a connection to the iRMC S2/S3 of the server within a specified time, it is assumed that the boot process has not been successful.
You can specify an action to be performed if this happens.

Proceed as follows:

- Check or uncheck the option(s) under *Enabled* for the *Software Watchdog* and/or *Boot Watchdog*.
- If you have activated either of these options, you can configure the following settings after *Software Watchdog* and/or *Boot Watchdog*:

  Continue
  No action is performed when the watchdog has expired, i.e. the server continues to run. An entry is made in the event log.

  Reset
  The server management software triggers a system reset.

  Power Cycle
  The server is powered down and immediately powered up again.

- As appropriate, enter the time (in minutes) after which this action is to be performed following *after timeout delay*.

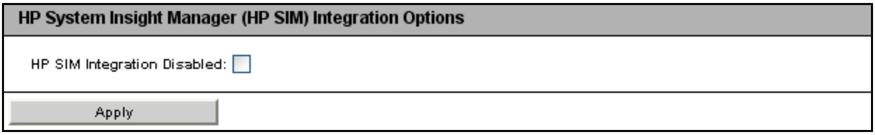
  i The boot watchdog must wait until the system has been started. You therefore have to specify a sufficient period for *after timeout delay (1 - 100)*.

- Click *Apply* button.

  The configured settings are saved and the actions which have been configured are performed in the appropriate circumstances.

HP System Insight Manager (HP SIM) Integration Options - Configure HP SIM integration

The *HP System Insight Manager (HP SIM) Integration Options* group allows you to configure whether the iRMC S2/S3 device will return some identifying information in response to an unauthenticated XML query sent from the HP System Insight Manager.



HP System Insight Manager (HP SIM) Integration Options

HP SIM Integration Disabled: □

Figure 135: Page Server Management Information - HP SIM Integration Options

Proceed as follows:

- Activate/deactivate the *HP SIM Integration Disabled* option in order to deactivate or to activate HP SIM integration.
- Click *Apply* to activate your settings.

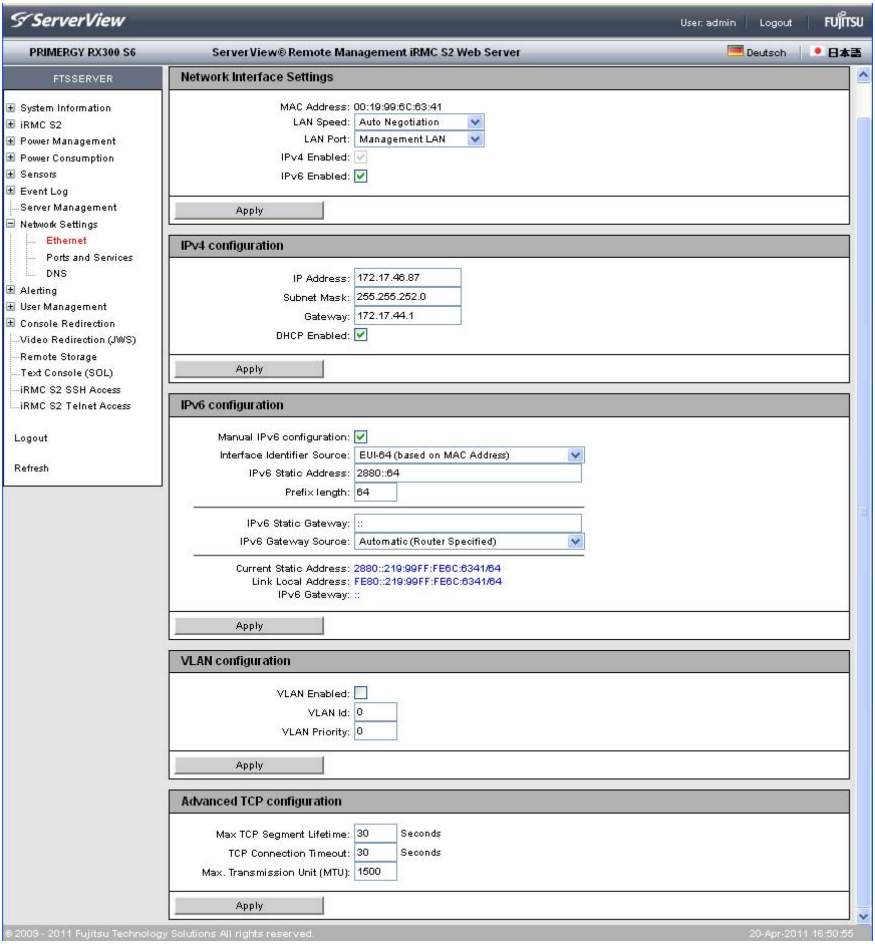
7.12 Network Settings - Configure the LAN parameters

The *Network Settings* entry brings together the links to the pages you use to configure the LAN parameters of the iRMC S2/S3:

- "Network Interface Settings - Configure Ethernet settings on the iRMC S2/S3" on page 239.
- "Ports and Network Services - Configuring ports and network services" on page 245.
- "DNS Configuration - Configuring DNS for the iRMC S2/S3" on page 249.

7.12.1 Network Interface Settings - Configure Ethernet settings on the iRMC S2/S3

The *Network Interface* page allows you to view and change the Ethernet settings for the iRMC S2/S3.



Network Interface Settings

MAC Address: 00:19:99:6C:63:41
LAN Speed: Auto Negotiation
LAN Port: Management LAN
IPv4 Enabled: ☑
IPv6 Enabled: ☑

IPv4 configuration

IP Address: 172.17.46.87
Subnet Mask: 255.255.252.0
Gateway: 172.17.44.1
DHCP Enabled: ☑

IPv6 configuration

Manual IPv6 configuration: ☑
Interface Identifier Source: EUI-64 (based on MAC Address)
IPv6 Static Address: 2880::64
Prefix length: 64

IPv6 Static Gateway: ::
IPv6 Gateway Source: Automatic (Router Specified)

Current Static Address: 2880::219:99FF:FE6C:6341/64
Link Local Address: FE80::219:99FF:FE6C:6341/64
IPv6 Gateway: ::

VLAN configuration

VLAN Enabled: □
VLAN Id: 0
VLAN Priority: 0

Advanced TCP configuration

Max TCP Segment Lifetime: 30 Seconds
TCP Connection Timeout: 30 Seconds
Max. Transmission Unit (MTU): 1500

Figure 136: Network Interface page

CAUTION!

Contact the network administrator responsible for the system before you change the Ethernet settings.

If you make illegal Ethernet settings for the iRMC S2/S3, you will only be able to access the iRMC S2/S3 using special configuration software, the serial interface or via the BIOS.

Only users with the *Configure iRMC S2/S3 Settings* permission are allowed to edit Ethernet settings (see chapter "User management for the iRMC S2/S3" on page 65).

Network Interface Settings

MAC Address

The MAC address of the iRMC S2/S3 is displayed here.

LAN Speed

LAN speed. The following options are available:

- Auto Negotiation
- 1000 MBit/s Full Duplex (depending on the server hardware)
- 100 MBit/s Full Duplex
- 100 MBit/s Half Duplex
- 10 MBit/s Full Duplex
- 10 MBit/s Half Duplex

If *Auto Negotiation* is selected, the onboard LAN controller assigned to the iRMC S2/S3 autonomously determines the correct transfer speed and duplex method for the network port it is connected to.

LAN Port

This option is not supported for all PRIMERGY servers.

On some PRIMERGY server models, the LAN interface of the installed system NIC (network interface card) can be set up

- as shared LAN for shared operation with the system

  or

- as a service LAN for exclusive use as a management LAN.

IPv4 Enabled

Enables/disables IPv4 addressing for the iRMC S2/S3. If IPv4 addressing is enabled, the *IPv4 configuration* group will be displayed (see below).

You cannot disable IPv4 addressing if the iRMC S2/S3 is currently accessed via IPv4.

IPv6 Enabled

Enables/disables IPv6 addressing for the iRMC S2/S3. If IPv6 addressing is enabled, the *IPv6 configuration* group will be displayed (see below).

You cannot disable IPv6 addressing if the iRMC S2/S3 is currently accessed via IPv6.

IPv4 configuration

The *IPv4 configuration* group allows you to configure the IPv4 settings for the iRMC S2/S3.

IP Address

IPv4 address of the iRMC S2/S3 in the LAN. This address is different from the IP address of the managed server.

> i If you are working with a static address (*DHCP enable* option not activated) then you can enter this here. Otherwise (if the *DHCP enable* option is activated), the iRMC S2/S3 only uses the field to display the address.

Subnet Mask

Subnet mask of the iRMC S2/S3 in the LAN.

Gateway

IPv4 address of the default gateway in the LAN.

DHCP Enabled

If you activate this option, the iRMC S2/S3 gets its LAN settings from a DHCP server on the network.

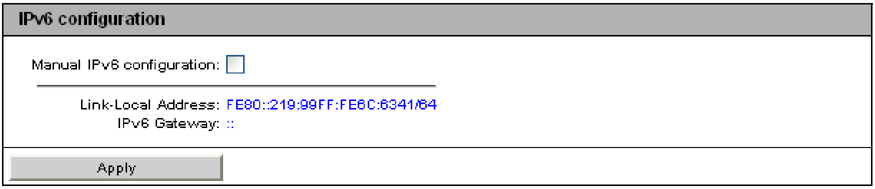
> i Do not activate the *DHCP* option if no DHCP server is available on the network.
> If you activate the *DHCP* option and there is no DHCP server available on the network, the iRMC S2/S3 goes into a search loop (i.e. it continues searching for a DHCP server until it finds one).

The (configured) iRMC S2/S3 can be registered with a DNS server by an appropriately configured DHCP server (see section "DNS Configuration - Configuring DNS for the iRMC S2/S3" on page 249).

IPv6 configuration

The *IPv6 configuration* group allows you to manually configure an IPv6 address for the iRMC S2/S3 in addition to the link-local address, which is always assigned automatically to the iRMC S2/S3 by using stateless autoconfiguration.

With ipv6 addressing, DHCP is not supported for the iRMC S2/S3.



IPv6 configuration

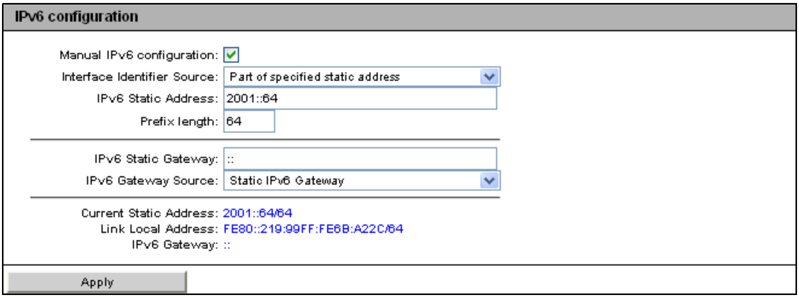
Manual IPv6 configuration: □

Link-Local Address: FE80::219:99FF:FE6C:6341/64
IPv6 Gateway: ::

Figure 137: Network Interface page - manual IPv6 configuration disabled

Manual IPv6 configuration

This option is disabled by default.
If you enable the *Manual IPv6 configuration* option, the *IPv6 configuration* group displays additional parameters that allow you to manually configure a routable IPv6 address for the iRMC S2/S3:



IPv6 configuration

Manual IPv6 configuration: ☑
Interface Identifier Source: Part of specified static address
IPv6 Static Address: 2001::64
Prefix length: 64

IPv6 Static Gateway: ::
IPv6 Gateway Source: Static IPv6 Gateway

Current Static Address: 2001::64/64
Link Local Address: FE80::219:99FF:FE6B:A22C/64
IPv6 Gateway: ::

Figure 138: Network Interface page - manual IPv6 configuration

Interface Identifier Source

Specifies from which source the interface identifier part of the IPv6 address is taken.

Part of the specified static address

Part of the static address specified under *IPv6 Static Address*.

EUI-64 (based on MAC address)

EUI-64 standard conform representation of the MAC address of the iRMC S2/S3.

IPv6 Static Address

Static IPv6 address for the iRMC S2/S3.

Prefix Length

Length of the IPv6 prefix.

IPv6 Static Gateway

Static IPv6 address of the default IPv6 gateway in the LAN.

IPv6 Gateway Source

IPv6 gateway that is used by the iRMC S2/S3.

Static IPv6 Gateway

Gateway specified under *IPv6 Static Gateway*.

Automatic (Router specific)

The gateway is determined automatically by the Router.

VLAN Configuration

*VLAN Enable*d

This option allows you to activate VLAN support for the iRMC S2/S3.

VLAN Id

VLAN ID of the virtual network (VLAN) the iRMC S2/S3 belongs to.
Permitted value range: 1 ≤ *VLAN Id* ≤ 4094.

VLAN Priority

VLAN priority (user priority) of the iRMC S2/S3 in the VLAN specified by *VLAN Id*.
Permitted value range: 0 ≤ *VLAN Priority* ≤ 7 (default: 0).

Advanced TCP configuration

Max TCP Segment Lifetime
Maximum lifetime (in seconds) of TCP/IP packet (Default: 32 seconds).

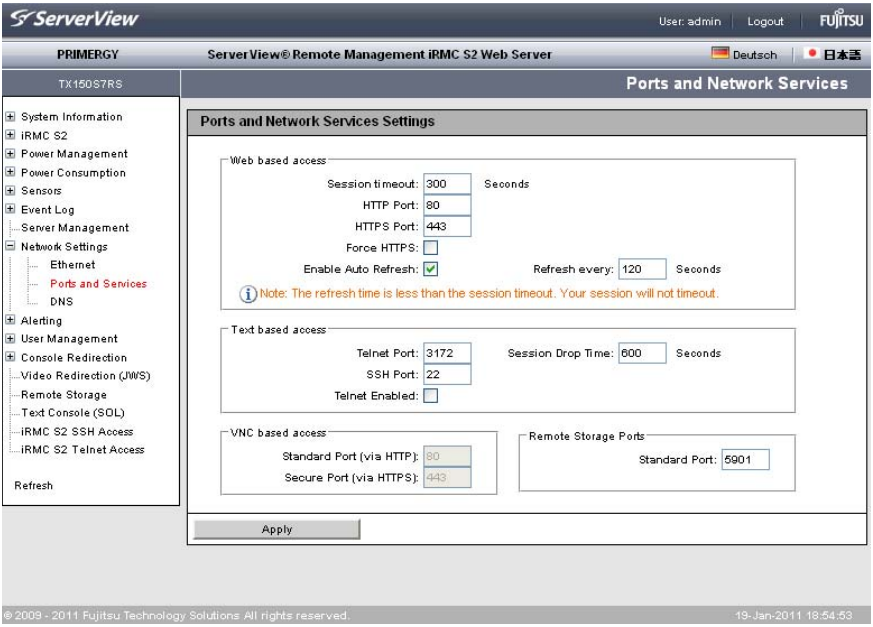
TCP Connection Timeout
Timeout value (in seconds) of the TCP connection (Default: 32 seconds).

Max. Transmission Unit (MTU)
Maximum packet size (in bytes) of the TCP/IP data packages that will be accepted by the TCP/IP connection. (Default: 3000 Bytes).

► Click *Apply* to activate the configured Ethernet settings.

7.12.2 Ports and Network Services - Configuring ports and network services

The *Ports and Network Services* page allows you to view and modify the configuration settings for ports and network services.



Ports and Network Services Settings

Web based access

Session timeout: 300 Seconds
HTTP Port: 80
HTTPS Port: 443
Force HTTPS: □
Enable Auto Refresh: ☑ Refresh every: 120 Seconds

Note: The refresh time is less than the session timeout. Your session will not timeout.

Text based access

Telnet Port: 3172 Session Drop Time: 600 Seconds
SSH Port: 22
Telnet Enabled: □

VNC based access

Standard Port (via HTTP): 80
Secure Port (via HTTPS): 443

Remote Storage Ports

Standard Port: 5901

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved. 19-Jan-2011 18:54:53

Figure 139: Ports and Network Services page

i Configuration is not supported for ports where the input fields are deactivated in the iRMC S2/S3 web interface.

Ports for web-based access

Session Timeout

Period of inactivity (in seconds) after which the session is automatically closed. The login page of the iRMC S2/S3 web interface then appears, and you can log in again as required (see page 136).

> i Your session will not automatically be closed if it is inactive when the time specified in *Session Timeout* has elapsed if you enter a value for the refresh interval which is less than the *Session Timeout* in the *Refresh every ... seconds* field (see page 247).

HTTP Port

HTTP port of the iRMC S2/S3
Default port number: 80
Configurable: yes
Enabled by default: yes
Communication direction: inbound and outbound

HTTPS Port

HTTPS (HTTP Secure) port of the iRMC S2/S3
Default port number: 443
Configurable: yes
Enabled by default: yes
Communication direction: inbound and outbound

Force HTTPS

If you enable the *Force HTTPS* option, users can only establish a secure connection to the iRMC S2/S3 on the HTTPS port specified in the entry field.

If you disable the *Force HTTPS* option, users can establish a non-secure connection to the iRMC S2/S3 on the HTTP port specified in the entry field.

> i If the SSL certificate has expired, a message to this effect is issued in the browser.

Enable Auto Refresh

If you activate this option, the contents of the iRMC S2/S3 web interface are automatically refreshed periodically. Specify the refresh interval in the *Refresh every ... seconds* field.

Refresh every ... seconds

Length (in seconds) of the interval for automatically refreshing the iRMC S2/S3 web interface.

If you enter a value for the refresh interval which is less than the *Session Timeout* (see page 246), your session will not automatically be closed when the time specified in *Session Timeout* has elapsed in the event of inactivity.

Ports for text-based access

Telnet Port

Telnet port of the iRMC S2/S3
Default port number: 3172
Configurable: yes
Enabled by default: no
Communication direction: inbound and outbound

Session Drop Time

Period of inactivity (in seconds) after which a Telnet connection is automatically cleared.

SSH Port

SSH (Secure Shell) port of the iRMC S2/S3
Default port number: 22
Configurable: yes
Enabled by default: yes
Communication direction: inbound and outbound

Telnet enabled

If you enable the *Telnet Enabled* option, users can establish a connection to the iRMC S2/S3 on the Telnet port specified in the entry field.

VNC ports

Standard Port

VNC port of the iRMC S2/S3 for secure and non-secure Advanced Video Redirection (AVR)
Port number: 80
Hard-configured
Enabled by default: yes
Communication direction: inbound

Secure Port (SSL)

VNC port of the iRMC S2/S3 for the SSL-secured transfer of mouse and keyboard input for AVR.
Port number: 443
Hard-configured.
Enabled by default: yes
Communication direction: inbound

Remote Storage Ports

Standard Port

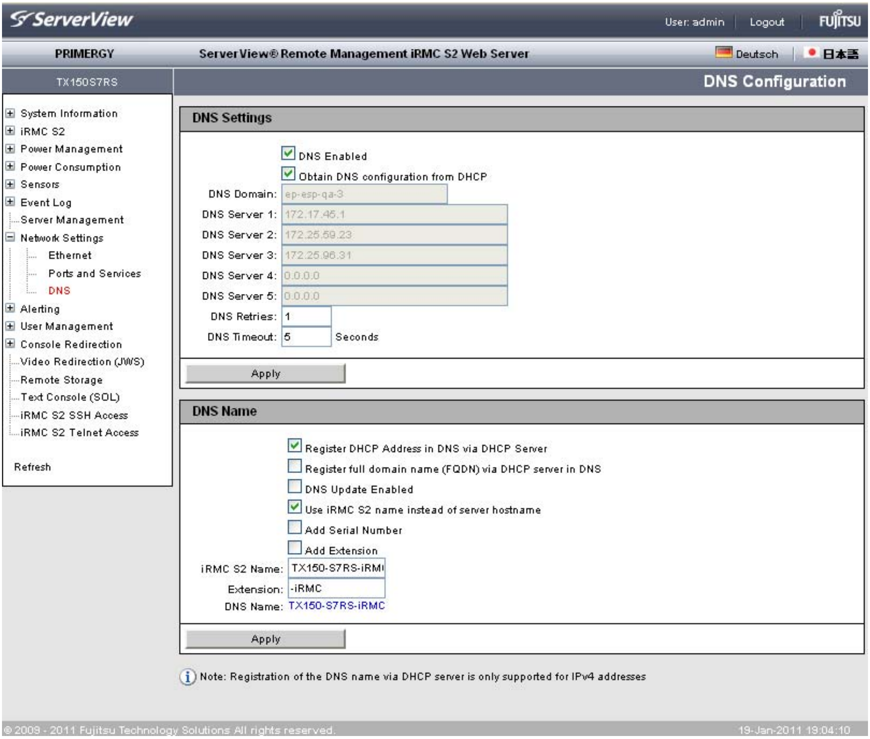
Default remote storage port of the iRMC S2/S3
Default port number: 5901
Configurable: yes
Enabled by default: yes
Communication direction: outbound to the remote workstation

i As of iRMC S2/S3 firmware version 5.00, the Remote Storage port is used only for the Remote Storage server and client-internal communications. For integrated Remote Storage, the http port is used.

► Click *Apply* to store the configured settings.

7.12.3 DNS Configuration - Configuring DNS for the iRMC S2/S3

The *DNS Configuration* page allows you to activate the Domain Name Service (DNS) for the iRMC S2/S3 and to configure a host name for the iRMC S2/S3.



DNS Settings

☑ DNS Enabled

☑ Obtain DNS configuration from DHCP

DNS Domain: ep-esp-qa-3

DNS Server 1: 172.17.45.1

DNS Server 2: 172.25.59.23

DNS Server 3: 172.25.96.31

DNS Server 4: 0.0.0.0

DNS Server 5: 0.0.0.0

DNS Retries: 1

DNS Timeout: 5 Seconds

DNS Name

☑ Register DHCP Address in DNS via DHCP Server

□ Register full domain name (FQDN) via DHCP server in DNS

□ DNS Update Enabled

☑ Use iRMC S2 name instead of server hostname

□ Add Serial Number

□ Add Extension

iRMC S2 Name: TX150-S7RS-iRM(

Extension: -iRMC

DNS Name: TX150-S7RS-iRMC

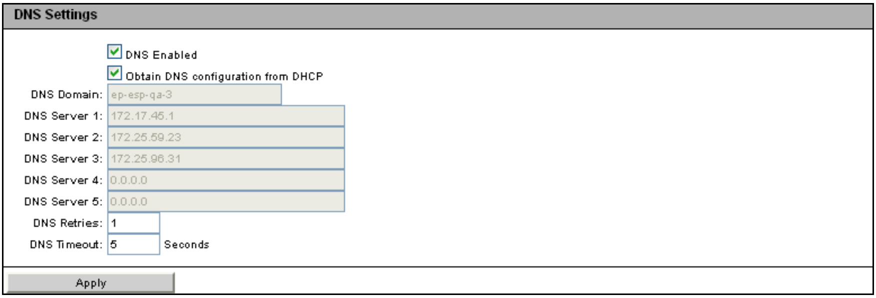
Note: Registration of the DNS name via DHCP server is only supported for IPv4 addresses

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.   19-Jan-2011 19:04:10

Figure 140: DNS Configuration page

DNS Settings

The *DNS Settings* group allows you to activate the Domain Name Service (DNS) for the iRMC S2/S3. This makes it possible to use symbolic DNS names instead of IP addresses for configuring the iRMC S2/S3.



DNS Settings

☑ DNS Enabled

☑ Obtain DNS configuration from DHCP

DNS Domain: ep-esp-qa-3

DNS Server 1: 172.17.45.1

DNS Server 2: 172.25.59.23

DNS Server 3: 172.25.96.31

DNS Server 4: 0.0.0.0

DNS Server 5: 0.0.0.0

DNS Retries: 1

DNS Timeout: 5 Seconds

Figure 141: DNS Configuration page - DNS Settings

DNS enabled

Enables/disables DNS for the iRMC S2/S3.

Obtain DNS configuration from DHCP

If you activate this option, the IP addresses of the DNS servers are obtained automatically from the DHCP server.
In this event, up to five DNS servers are supported.

If you do not enable this setting, you can enter up to five DNS server addresses manually under *DNS-Server 1* - *DNS-Server 5*.

DNS Domain

If the option *Obtain DNS configuration from DHCP* is disabled, specify the name of the default domain for requests to the DNS server(s).

DNS Server 1 .. 5

If the *Obtain DNS configuration from DHCP* option is disabled, you can enter the names of up to five DNS servers here.

DNS Retries

Number of DNS retries.

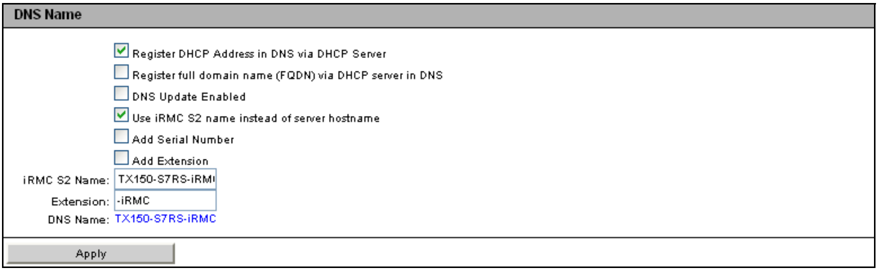
DNS Timeout

Timeout (in seconds) for a DNS response.

► Click *Apply* to store the configured settings.

DNS Name

The *DNS Name* group allows you to configure a host name for the iRMC S2/S3 and thus use “dynamic DNS”. Dynamic DNS allows DHCP servers to autonomously pass on the IP address and system name of a network component to DNS servers to facilitate identification.



DNS Name

☑ Register DHCP Address in DNS via DHCP Server
☐ Register full domain name (FQDN) via DHCP server in DNS
☐ DNS Update Enabled
☑ Use iRMC S2 name instead of server hostname
☐ Add Serial Number
☐ Add Extension

iRMC S2 Name: TX150-S7RS-iRMI
Extension: -iRMC
DNS Name: TX150-S7RS-iRMC

Figure 142: DNS Configuration page - DNS Name

Register DHCP Address in DNS via DHCP Server

This option is disabled if IPv6 addressing is used.
Enables/disables the transfer of the DHCP name to the DHCP server for the iRMC S2/S3 and the DNS registration via DHCP server.

Register full domain name (FQDN) via DHCP server in DNS

This option is disabled if IPv6 addressing is used.
Enables/disables the transfer of the FQDN (Fully Qualified Domain Name) to the DHCP server for the iRMC S2/S3 and the DNS registration via DHCP server.

DNS Update Enabled

Enables/disables update of DNS records via Dynamic DNS.

Use iRMC S2/S3 name instead of server hostname

The iRMC S2/S3 name specified in the *iRMC S2/S3 Name* entry field is used for the iRMC S2/S3 instead of the server name.

Add Serial Number

The last 3 bytes of the MAC address of the iRMC S2/S3 are appended to the DHCP name of the iRMC S2/S3.

Add Extension

The extension specified in the *Extension* entry field is appended to the DHCP name of the iRMC S2/S3.

iRMC S2/S3 Name

iRMC S2/S3 name passed to DHCP for the iRMC S2/S3 in place of the server name. Depending on the related options, the iRMC S2/S3 name is used as part of the DNS name.

Extension

Name extension for the iRMC S2/S3.

DNS Name

Shows the configured DNS name for the iRMC S2/S3.

► Click *Apply* to store the configured settings.

7.13 Alerting - Configure alerting

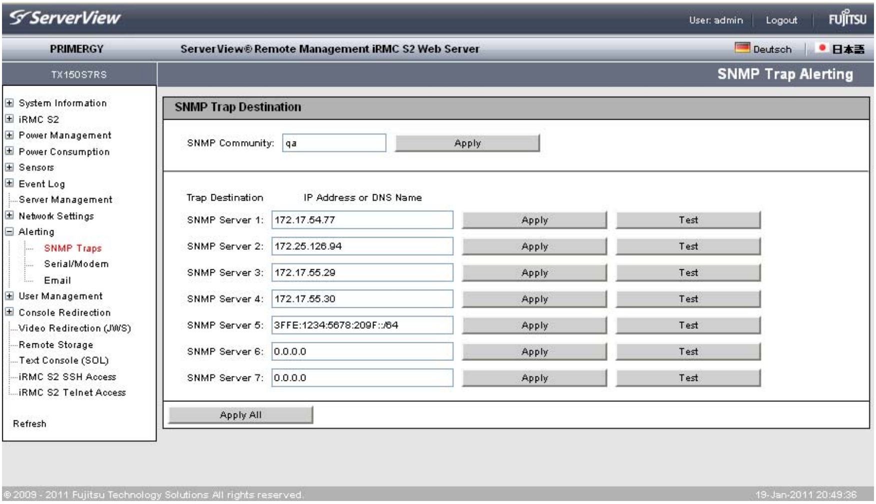
The *Alerting* entry contains the links to the pages you use to configure alerting for the iRMC S2/S3:

- "SNMP Trap Alerting - Configure SNMP trap alerting" on page 254.
- "Serial / Modem Alerting - Configure alerting via modem" on page 255.
- "Email Alerting - Configure email alerting" on page 257.

7.13.1 SNMP Trap Alerting - Configure SNMP trap alerting

The *SNMP Trap Alerting* page allows you to view and configure the settings for SNMP trap alerting.

> Forwarding of SNMP traps to up to seven SNMP servers is supported.



SNMP Trap Destination

SNMP Community: qa

Trap Destination	IP Address or DNS Name
SNMP Server 1:	172.17.54.77
SNMP Server 2:	172.25.126.94
SNMP Server 3:	172.17.55.29
SNMP Server 4:	172.17.55.30
SNMP Server 5:	3FFE:1234:5678:209F::/64
SNMP Server 6:	0.0.0.0
SNMP Server 7:	0.0.0.0

Figure 143: SNMP Trap Alerting page

SNMP Community

Name of the SNMP community.

- ► Click *Apply* to accept the community name.

SNMP Server1 .. SNMP Server7 (trap destinations)

DNS names or IP addresses of the servers that belong to this community and are to be configured as *Trap Destinations*.

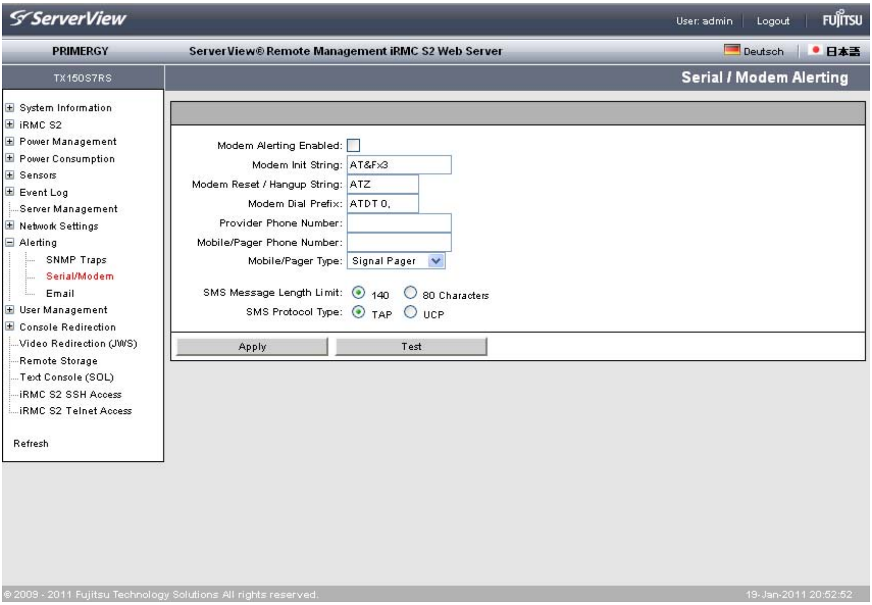
- ► Click *Apply* to activate the SNMP server as a trap destination.
- ► Click *Test* to test the connection to the SNMP server.

► Click *Apply All* to activate all the settings if appropriate.

7.13.2 Serial / Modem Alerting - Configure alerting via modem

The *Serial / Modem Alerting* page is only available with the iRMC S2.

The *Serial / Modem Alerting* page allows you to configure how alerts are forwarded via a modem.



Modem Alerting Enabled: □
Modem Init String: AT&Fx3
Modem Reset / Hangup String: ATZ
Modem Dial Prefix: ATDT 0,
Provider Phone Number:
Mobile/Pager Phone Number:
Mobile/Pager Type: Signal Pager
SMS Message Length Limit: ● 140 ○ 80 Characters
SMS Protocol Type: ● TAP ○ UCP

Figure 144: Serial / Modem Alerting page

Modem Alerting Enable

Enables or disables serial / modem alerting.

Modem Init String

Please refer to your modem documentation for details on this entry.

Modem Reset/Hangup String

Please refer to your modem documentation for details on this entry.

Modem Dial Prefix

This entry will depend on the type of connection you have.

Provider Phone Number

Enter the name of the SMS server.

Handy/Pager Phone Number

Enter the name of the mobile phone.

Handy/Pager Type

You can choose between:

- Signal Pager
- Numeric Pager
- Alpha pager
- SMS
- DoCoMo

SMS Message Length Limit

You can choose between 80 or 140 as the maximum length.

SMS Protocol Type

Enable the option corresponding to the mobile phone network used.

► Click *Apply* to activate your settings.

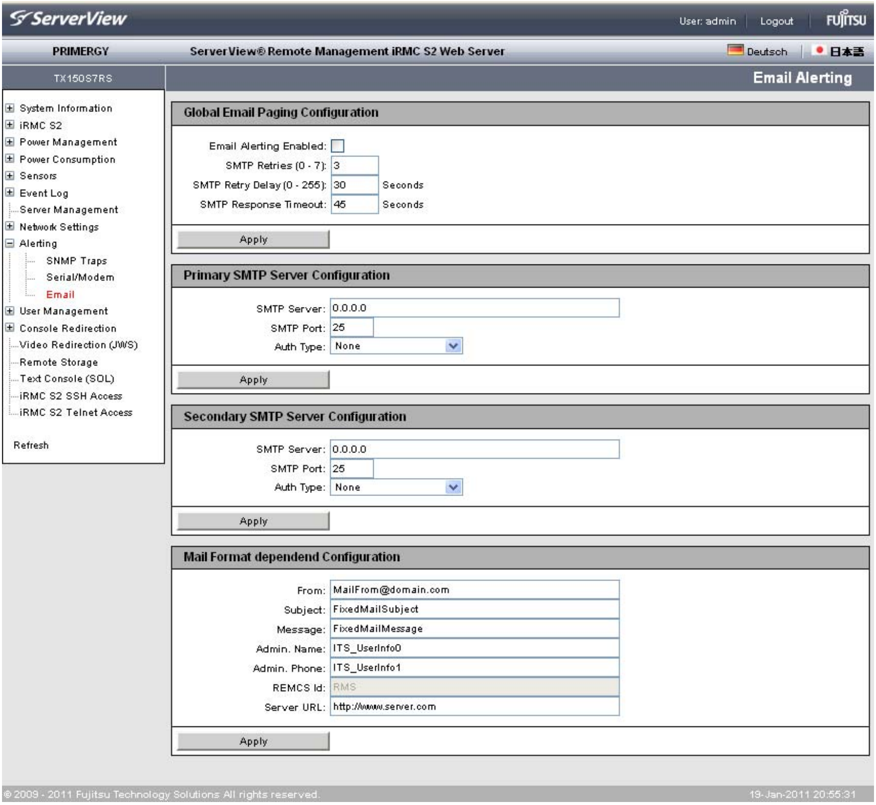
► Click *Test* to send a test alert.

7.13.3 Email Alerting - Configure email alerting

The *Email Alerting* page allows you to configure the settings for email alerting.

Configuration of two mail servers is supported.

Email alerting can be specified individually for each user (see section "User “<name>” Configuration - User configuration (details)" on page 266).



Global Email Paging Configuration

Email Alerting Enabled: □
SMTP Retries (0 - 7): 3
SMTP Retry Delay (0 - 255): 30 Seconds
SMTP Response Timeout: 45 Seconds

Primary SMTP Server Configuration

SMTP Server: 0.0.0.0
SMTP Port: 25
Auth Type: None

Secondary SMTP Server Configuration

SMTP Server: 0.0.0.0
SMTP Port: 25
Auth Type: None

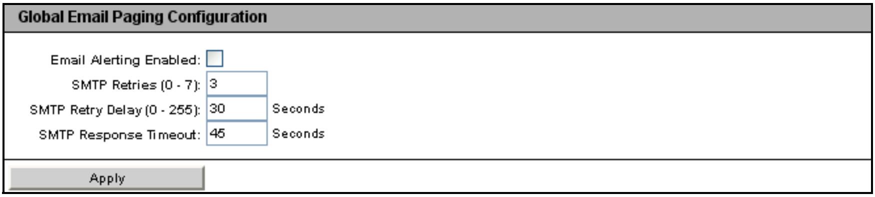
Mail Format dependend Configuration

From: MailFrom@domain.com
Subject: FixedMailSubject
Message: FixedMailMessage
Admin. Name: ITS_UserInfo0
Admin. Phone: ITS_UserInfo1
REMCS Id: RMS
Server URL: http://www.server.com

Figure 145: Email Alerting page

Global Email Paging Configuration - Configure global email settings

The *Global Email Paging Configuration* group allows you to configure the global email settings.



Global Email Paging Configuration

Email Alerting Enabled: □

SMTP Retries (0 - 7): 3

SMTP Retry Delay (0 - 255): 30 Seconds

SMTP Response Timeout: 45 Seconds

Figure 146: Email Alerting page, Global Email Configuration

Email Alerting Enable
Activate this option.

SMTP Retries (0 - 7)
Number of SMTP retries.

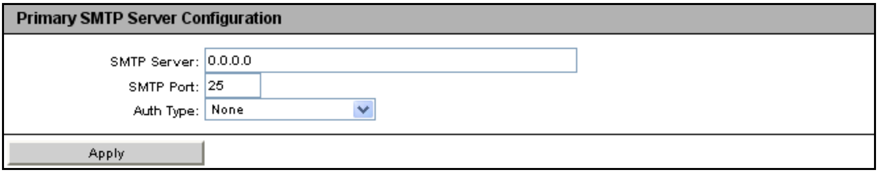
SMTP Retry Delay (0 - 255)
Time (in seconds) between SMTP retries.

SMTP Response Timeout
Timeout (in seconds) for an SMTP response.

► Click *Apply* to activate your settings.

Primary SMTP Server Configuration - Configure primary mail server

The *Primary SMTP Server Configuration* group allows you to configure the primary server (SMTP server).



Primary SMTP Server Configuration

SMTP Server: 0.0.0.0

SMTP Port: 25

Auth Type: None

Figure 147: Email Alerting page, Primary SMTP Server Configuration

SMTP Server

IP address of the primary mail server

> i You can activate the Domain Name Service (DNS) for the iRMC S2/S3 (see "DNS Configuration - Configuring DNS for the iRMC S2/S3" on page 249). You can then use a symbolic name instead of the IP address.

SMTP Port

SMTP port of the mail server

Auth Type

Authentication type for connecting the iRMC S2/S3 to the mail server:

– *None*
  No authentication for the connection.

– *SMTP AUTH (RFC 2554)*
  Authentication according to RFC 2554: SMTP Service Extension for Authentication.

  In this case, the following information is required:

  Auth User Name
  User name for authentication on the mail server

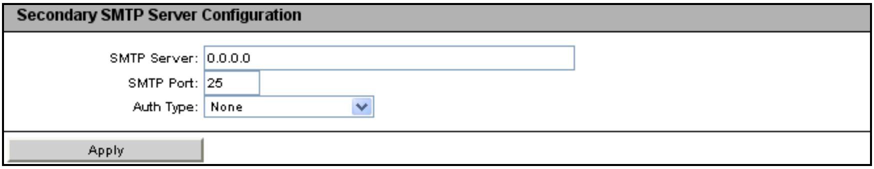
  Auth Password
  Password for authentication on the mail server

  Confirm Password
  Confirm the password entered.

► Click *Apply* to activate your settings.

Secondary SMTP Server Configuration - Configure secondary mail server

The *Secondary SMTP Server Configuration* group allows you to configure the secondary server (SMTP server).



Secondary SMTP Server Configuration

SMTP Server: 0.0.0.0
SMTP Port: 25
Auth Type: None

Figure 148: Email Alerting page - Secondary SMTP Server Configuration

SMTP Server

IP address of the secondary mail server

i You can activate the Domain Name Service (DNS) for the iRMC S2/S3 (see "DNS Configuration - Configuring DNS for the iRMC S2/S3" on page 249). You can then use a symbolic name instead of the IP address.

SMTP Port

SMTP port of the mail server

Auth Type

Authentication type for connecting the iRMC S2/S3 to the mail server:

- *None*
  No authentication for the connection.

- *SMTP AUTH (RFC 2554)*
  Authentication according to RFC 2554: SMTP Service Extension for Authentication.

  In this case, the following information is required:

  Auth User Name
  User name for authentication on the mail server

  Auth Password
  Password for authentication on the mail server

  Confirm Password
  Confirm the password entered.

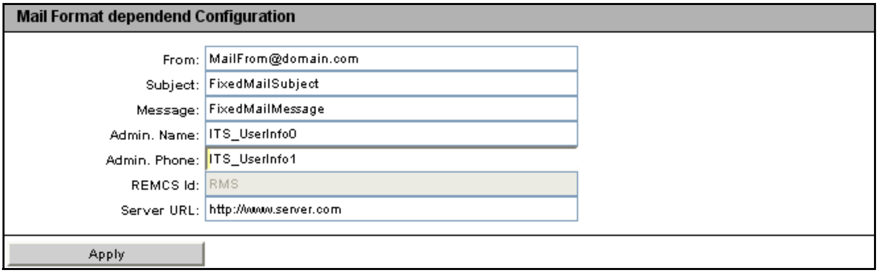
► Click *Apply* to activate your settings.

Mail Format dependent Configuration - Configure mail-format-dependent settings

The *Mail Format dependent Configuration* group allows you to configure the mail-format-dependent settings. You specify the mail format for each user using the *New User Configuration* - *User <Name> Configuration* - *Email Format Configuration* page (see page 270).

The following email formats are supported:

- Standard
- Fixed Subject
- ITS-Format
- Fujitsu REMCS Format



Mail Format dependend Configuration

From:	MailFrom@domain.com
Subject:	FixedMailSubject
Message:	FixedMailMessage
Admin. Name:	ITS_UserInfo0
Admin. Phone:	ITS_UserInfo1
REMCS Id:	RMS
Server URL:	http://www.server.com

Figure 149: Email Alerting page, Mail Format dependent Configuration

Some entry fields are disabled depending on the mail format.

From

Sender identification iRMC S2/S3.
Active for all mail formats.

> If the string entered here contains an "@", the string is interpreted as a valid email address. Otherwise, "admin@<ip-address>" is used as the valid email address.

Subject

Fixed subject for the alert mails.
Only active for the *Fixed Subject* mail format (see page 270).

Message

Type of message (email).
Only active for the *Fixed Subject* mail format (see page 270).

Admin Name

Name of the administrator responsible (optional).
Only active for the *ITS* mail format (see page 270).

Admin Phone

Phone number of the administrator responsible (optional).
Only active for the *ITS* mail format (see page 270).

REMCS Id

This ID is an additional server ID, similar to the serial number.
Only active for the mail format *Fujitsu REMCS-Format*.

Server URL

A URL under which the server is accessible under certain conditions. You have to enter the URL manually.
Only active for the *Standard* mail format.

► Click *Apply* to store your settings.

7.14 User Management

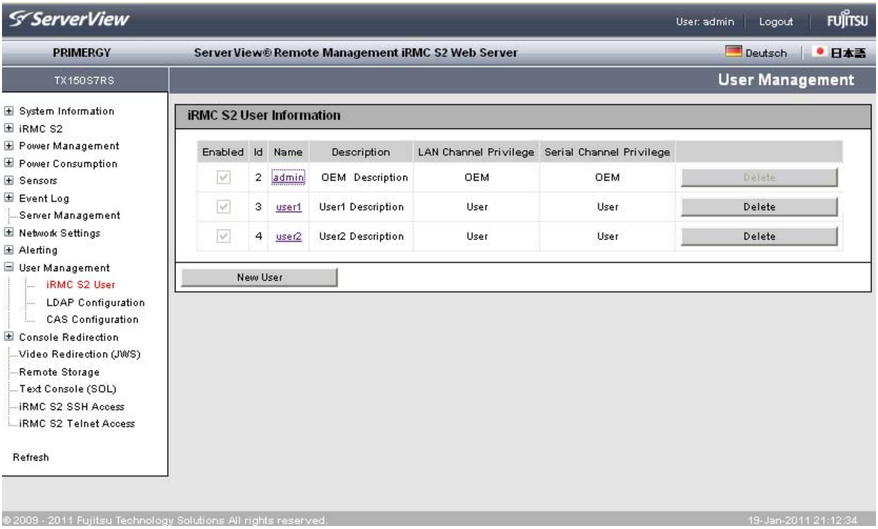
The *User Management* entry contains the links to the pages for local user management as well as for the configuration of the directory service for global user management (LDAP configuration):

- "iRMC S2/S3 User - local user management on the iRMC S2/S3" on page 263.
- "Directory Service Configuration (LDAP) - Configuring the directory service at the iRMC S2/S3" on page 273.
- "Centralized Authentication Service (CAS) Configuration - Configuring the CAS Service" on page 286.

7.14.1 iRMC S2/S3 User - local user management on the iRMC S2/S3

The *iRMC S2/S3 User* page contains a table showing all the configured users: Each line contains the data for one configured user. The user names are implemented in the form of links. Clicking on a user name opens the *User "<name>" Configuration* window (see page 266), in which you can view or modify the settings for this user.

i User ID 1 ("null user") is reserved for the IPMI standard and is therefore unavailable for user management on the iRMC S2/S3.



iRMC S2 User Information

Enabled	Id	Name	Description	LAN Channel Privilege	Serial Channel Privilege	
☑	2	admin	OEM Description	OEM	OEM	Delete
☑	3	user1	User1 Description	User	User	Delete
☑	4	user2	User2 Description	User	User	Delete

Figure 150: User Management page

Delete

The table of configured users includes a *Delete* button after each user entry. Click this button to delete the associated user after confirming this choice.

New User

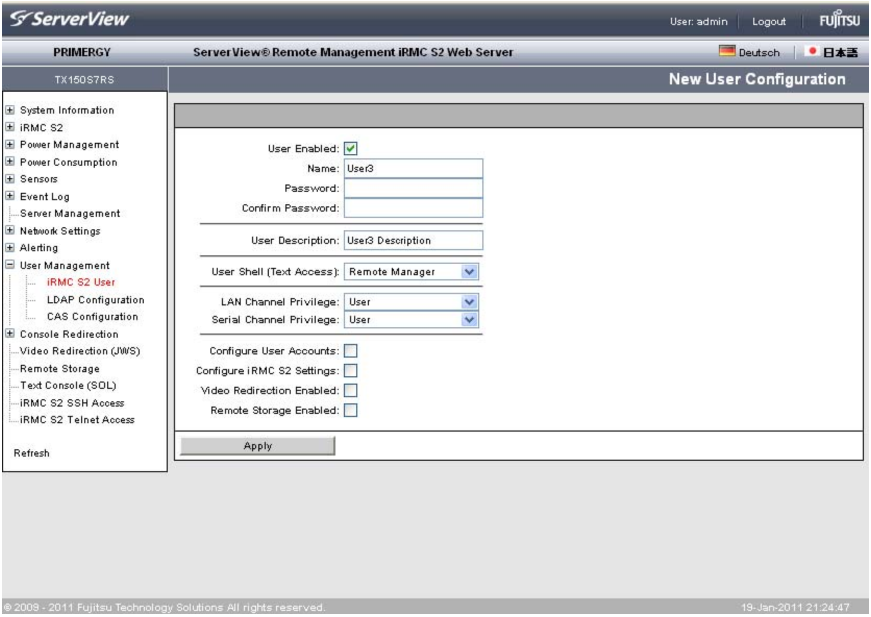
When you click this button, the *New User Configuration* page opens (see page 265). You can configure a new user here.

7.14.1.1 New User Configuration - Configuring a new user

The *New User Configuration* page allows you to configure the basic settings for a new user.

You will find explanations of the fields and selection lists on the *New User Configuration* page as of page 267 under the description of the *User "<name>" Configuration* page.

In figure 151 you can see the configuration of a user with the name "User3".



User Enabled: ☑
Name: User3
Password:
Confirm Password:

User Description: User3 Description

User Shell (Text Access): Remote Manager

LAN Channel Privilege: User
Serial Channel Privilege: User

Configure User Accounts: □
Configure iRMC S2 Settings: □
Video Redirection Enabled: □
Remote Storage Enabled: □

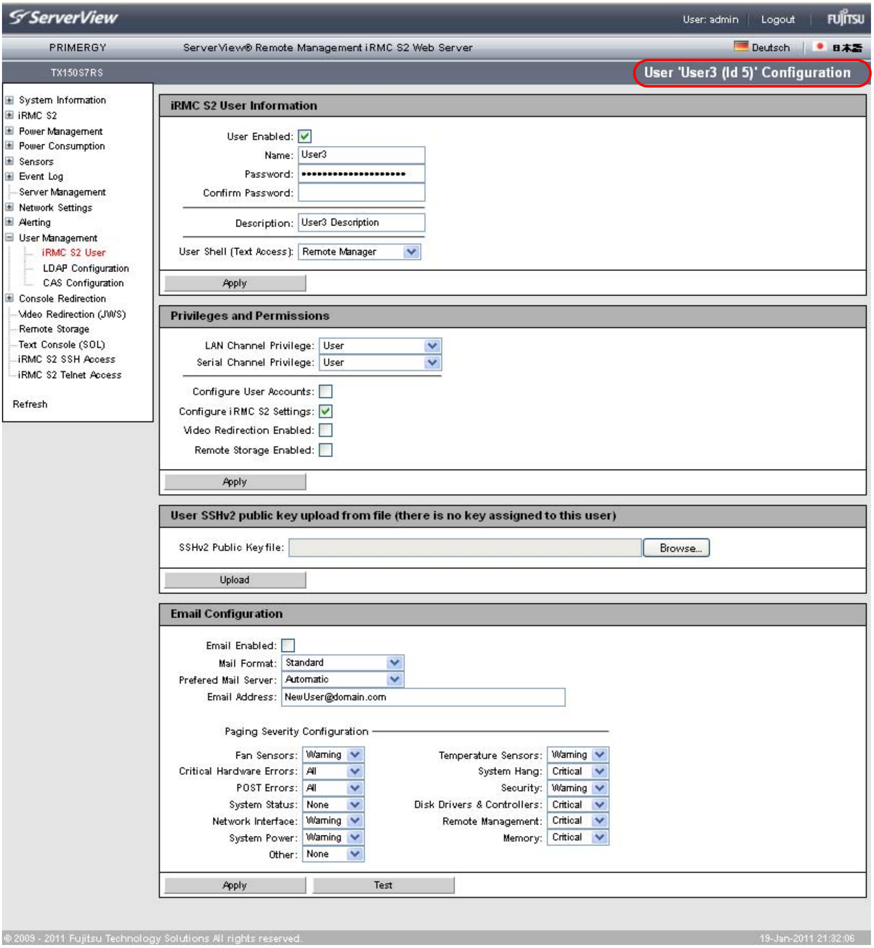
Figure 151: User Management - New User Configuration page

7.14.1.2 User “<name>” Configuration - User configuration (details)

The *User “<name>” Configuration* page allows you to view, modify and extend the settings for a user.

In figure 152 you can see the configuration of the user created in figure 151.

The user ID is shown in brackets after the user name.



User 'User3 (Id 5)' Configuration

iRMC S2 User Information

User Enabled: ☑
Name: User3
Password: ********************
Confirm Password:
Description: User3 Description
User Shell (Text Access): Remote Manager

Privileges and Permissions

LAN Channel Privilege: User
Serial Channel Privilege: User
Configure User Accounts: □
Configure iRMC S2 Settings: ☑
Video Redirection Enabled: □
Remote Storage Enabled: □

User SSHv2 public key upload from file (there is no key assigned to this user)

SSHv2 Public Key file:

Email Configuration

Email Enabled: □
Mail Format: Standard
Prefered Mail Server: Automatic
Email Address: NewUser@domain.com

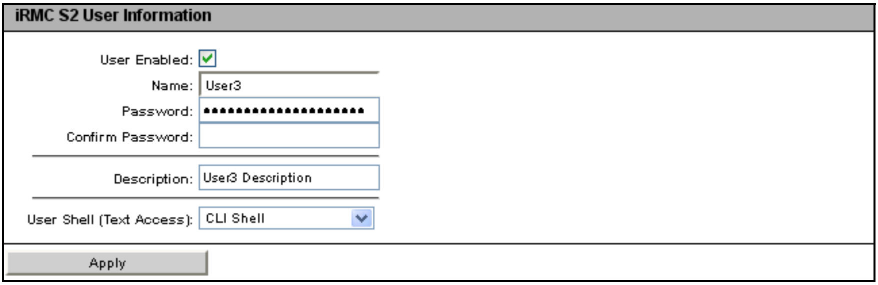
Paging Severity Configuration

Fan Sensors:	Warning	Temperature Sensors:	Warning
Critical Hardware Errors:	All	System Hang:	Critical
POST Errors:	All	Security:	Warning
System Status:	None	Disk Drivers & Controllers:	Critical
Network Interface:	Warning	Remote Management:	Critical
System Power:	Warning	Memory:	Critical
Other:	None		

Figure 152: User Management - User “<name>” Configuration page

User Information - Configuring user access data

The *User Information* group allows you to configure the access data for the user.



iRMC S2 User Information

User Enabled: ☑

Name: User3

Password: ********************

Confirm Password:

Description: User3 Description

User Shell (Text Access): CLI Shell

Figure 153: User Management - User “<name>” Configuration page, User Information

User Enabled

Disable this option to lock the user.

Name

Enter the name of the user.

Password

Enter the user password.

Confirm Password

Confirm the password by entering it again here.

User Description

Enter a general description of the configured user here.

User Shell

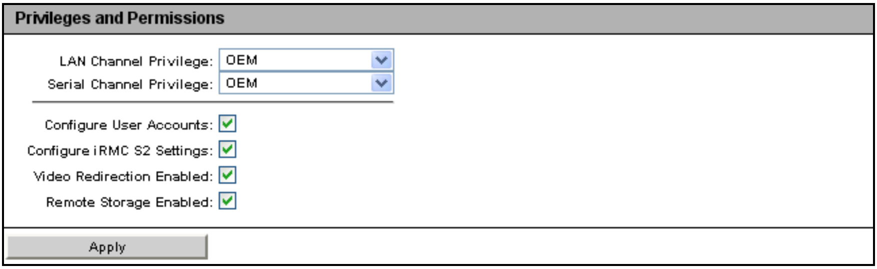
Select the desired user shell here.
The following options are available:

- *SMASH CLP*
  See section "Start a Command Line shell... - Start a SMASH CLP shell" on page 340.
- *Remote Manager*
  See chapter "iRMC S2/S3 via Telnet/SSH (Remote Manager)" on page 321.
- *IPMI Terminal Mode*
- *None*

► Click *Apply* to activate your settings.

Privileges / Permissions - Assigning user privileges

The *Privileges / Permissions* group allows you to configure the channel-specific user privileges.



Privileges and Permissions

LAN Channel Privilege: OEM

Serial Channel Privilege: OEM

Configure User Accounts: ☑

Configure iRMC S2 Settings: ☑

Video Redirection Enabled: ☑

Remote Storage Enabled: ☑

Figure 154: User Management - User “<name>” Configuration page, Privilege / Permissions

LAN Channel Privilege

Assign a privilege group for a LAN channel to the user here:

- *User*
- *Operator*
- *Administrator*
- *OEM*

Refer to section "User permissions" on page 68 for information on the permissions associated with the privilege groups.

Serial Channel Privilege

Assign a privilege group for a serial channel to the user here: The same privilege groups are available as for *LAN Channel Privilege*.

In addition to the channel-specific permissions, you can also individually assign users the following channel-independent permissions:

Configure User Accounts

Permission to configure local user access data.

Configure iRMC S2/S3 Settings

Permission to configure the iRMC S2/S3 settings.

Video Redirection enabled

Permission to use Advanced Video Redirection (AVR) in “View Only” and “Full Control” mode.

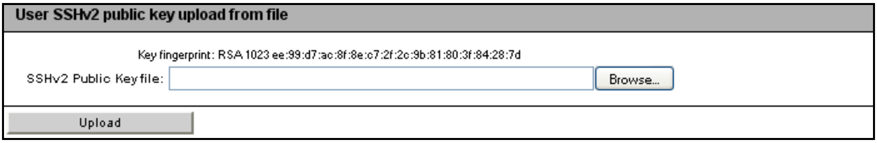
Remote Storage enabled

Permission to use the Remote Storage functionality.

► Click *Apply* to activate your settings.

User SSHv2 public key upload from file

The *User SSHv2 public Key uploag from file* group allows you to load an user SSHv2 public key from a local file.



User SSHv2 public key upload from file

Key fingerprint: RSA 1023 ee:99:d7:ac:8f:8e:c7:2f:2c:9b:81:80:3f:84:28:7d

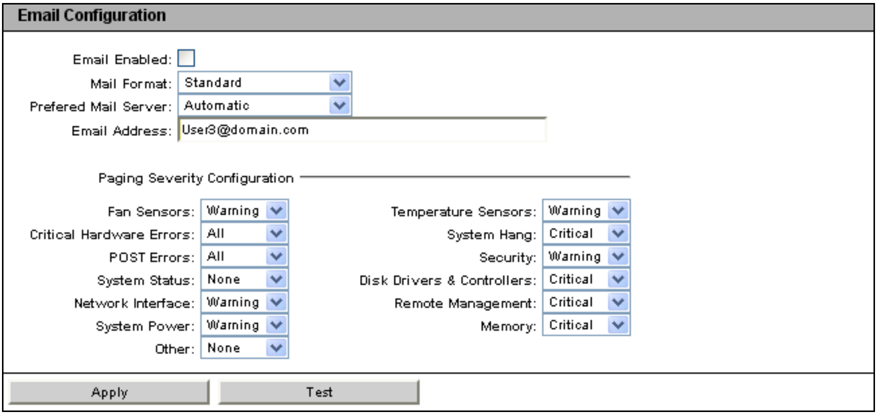
SSHv2 Public Key file:

Figure 155: User Management - User “<name>” Configuration page, User SSHv2 public key upload from file

For further details on SSHv2 public key authentication for iRMC S2/S3 users see section "SSHv2 public key authentication for iRMC S2/S3 users" on page 72.

Email Configuration - Configure user-specific email settings

The *Email Configuration* group allows you to configure the user-specific settings governing the email format.



Email Configuration

Email Enabled: □

Mail Format: Standard

Prefered Mail Server: Automatic

Email Address: User3@domain.com

Paging Severity Configuration

Fan Sensors:	Warning	Temperature Sensors:	Warning
Critical Hardware Errors:	All	System Hang:	Critical
POST Errors:	All	Security:	Warning
System Status:	None	Disk Drivers & Controllers:	Critical
Network Interface:	Warning	Remote Management:	Critical
System Power:	Warning	Memory:	Critical
Other:	None		

Figure 156: User Management - User “<name>” Configuration page, Email Configuration

Email Enabled

Specify whether the user is to be informed about system statuses by email.

Mail Format

Depending on the selected email format, you can make a number of settings in the *Email Alerting - Mail Format dependent Configuration group* (see page 261).

The following email formats are available:

- *Standard*
- *Fixed Subject*
- *ITS-Format*
- *Fujitsu REMCS Format*

Preferred Mail Server

Select the preferred mail server.
You can choose one of the following options:

– *Automatic*

  If the email cannot be sent successfully immediately, for instance because the preferred mail server is not available, the email is sent to the second mail server.

– *Primary*

  Only the mail server which has been configured as the primary SMTP server (see page 259) is used as the preferred mail server.

– *Secondary*

  Only the mail server which has been configured as the secondary SMTP server (see page 260) is used as the preferred mail server.

i Errors sending email are recorded in the event log.

Email Address

Email address of recipient.

Paging Severity Configuration

Here you can configure system events about which an iRMC S2/S3 user is to be informed by email.

i Every entry in the event log for the iRMC S2/S3 is assigned to a particular paging group.

The following settings are available for each event group:

None

The notification function is deactivated for this paging group.

Critical

The iRMC S2/S3 notifies users by email if an entry in the system event log is reported as *CRITICAL*.

Warning

The iRMC S2/S3 notifies users by email if an entry in the system event log is reported as *Minor* or *Major* or *Critical*.

All

The iRMC S2/S3 notifies users of every event in this group which causes an entry to be made in the system event log.

► Click *Apply* to activate your settings.

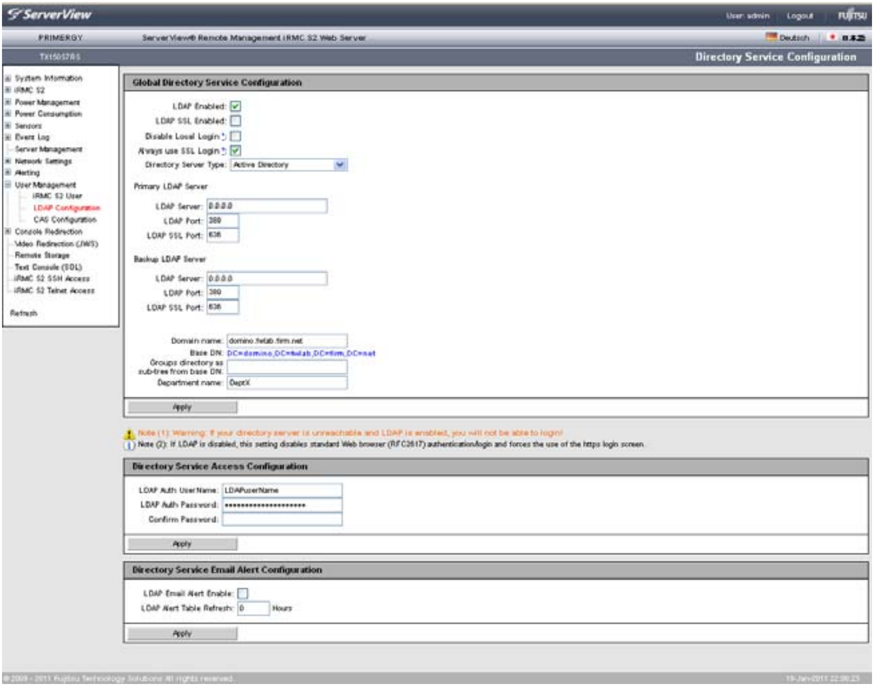
7.14.2 Directory Service Configuration (LDAP) - Configuring the directory service at the iRMC S2/S3

In order to perform global user management via a directory service (see the "User Management in ServerView" manual), you must configure the iRMC S2/S3 appropriately in the *Directory Service Configuration* page.

Currently, support for iRMC S2/S3 LDAP access is provided for the following directory services: Microsoft Active Directory, Novell eDirectory and Open LDAP.

The following characters are reserved as metacharacters for search strings in LDAP: *, \ , &, |, !, =, <, >, ~, :

You must therefore not use these characters as components of Relative Distinguished Names (RDN).



Global Directory Service Configuration

LDAP Enabled: ☑
LDAP SSL Enabled: □
Disable Local Login (1): □
Always use SSL Login (2): ☑
Directory Server Type: Active Directory

Primary LDAP Server
LDAP Server: 0.0.0.0
LDAP Port: 389
LDAP SSL Port: 636

Backup LDAP Server
LDAP Server: 0.0.0.0
LDAP Port: 389
LDAP SSL Port: 636

Domain name: domino.fwlab.firm.net
Base DN: DC=domino,DC=fwlab,DC=firm,DC=net
Groups directory as sub-tree from base DN:
Department name: DeptX

Note (1): Warning: If your directory server is unreachable and LDAP is enabled, you will not be able to login!
Note (2): If LDAP is disabled, this setting disables standard Web browser (RFC2617) authentication/login and forces the use of the https login screen.

Directory Service Access Configuration

LDAP Auth UserName: LDAPuserName
LDAP Auth Password: ********************
Confirm Password:

Directory Service Email Alert Configuration

LDAP Email Alert Enable: □
LDAP Alert Table Refresh: 0 Hours

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.
19-Jan-2011 22:09:23

Figure 157: Directory Service Configuration page (LDAP configuration)

LDAP Enabled

This option specifies whether the iRMC S2/S3 can access a directory service via LDAP. Directory service access via LDAP is only possible if *LDAP Enable* has been activated.

If *LDAP Enable* is checked then the login information (see page 136) is always transferred with SSL encryption between the web browser and the iRMC S2/S3.

LDAP SSL Enabled

If you check this option then data transfer between iRMC S2/S3 and the directory server is SSL encrypted.

LDAP SSL Enable has no influence on whether or not the iRMC S2/S3 web interface pages are SSL-protected on opening.

You should only activate *LDAP SSL Enable* if a domain controller certificate is installed.

Disable Local Login

If you activate this option then all the local iRMC S2/S3 user identifications are locked and only the user identifications managed by the directory service are valid.

CAUTION!

If the option *Disable Local Login* is activated and the connection to the directory service fails then it is no longer possible to log in at the iRMC S2/S3.

Always use SSL Login

This option is only relevant if LDAP is deactivated.

If you activate this option then the HTTP SSL-secured login page is always used even if LDAP is deactivated. Only if you do not activate *Always use SSL Login* and LDAP is deactivated is a mask secured via Digest Authentication Login used.

Directory Server Type

Type of directory server used:

The following directory services are supported:

- *Active Directory*: Microsoft Active Directory
- *Novell*: Novell eDirectory
- *OpenLDAP*: OpenLDAP
- *Open DS*

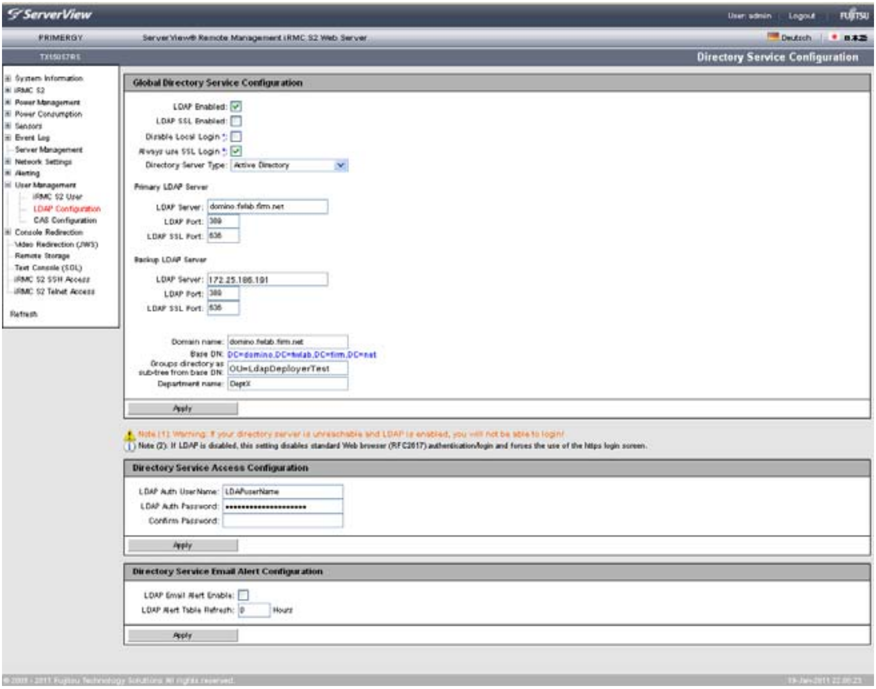
► Click *Apply* to activate your settings.

Different input fields are provided, depending on the directory service you select:

- For *Active Directory*, refer to section "Configuring iRMC S2/S3 for Microsoft Active Directory" on page 276.
- For *eDirectory*, *Open LDAP* and *OpenDS*, refer to section "Configuring iRMC S2/S3 for Novell eDirectory / OpenLDAP / OpenDS" on page 280.

7.14.2.1 Configuring iRMC S2/S3 for Microsoft Active Directory

After you have confirmed the *Active Directory* you have chosen by clicking *Apply*, the following variant of the *Directory Service Configuration* page is shown:



Global Directory Service Configuration

LDAP Enabled: ☑
LDAP SSL Enabled: □
Disable Local Login [1]: □
Always use SSL Login [1]: ☑
Directory Server Type: Active Directory

Primary LDAP Server

LDAP Server: domino.fwlab.firm.net
LDAP Port: 389
LDAP SSL Port: 636

Backup LDAP Server

LDAP Server: 172.25.186.191
LDAP Port: 389
LDAP SSL Port: 636

Domain name: domino.fwlab.firm.net
Base DN: DC=domino,DC=fwlab,DC=firm,DC=net
Groups directory as sub-tree from base DN: OU=LdapDeployerTest
Department name: DeptX

Note (1): Warning: If your directory server is unreachable and LDAP is enabled, you will not be able to login!
Note (2): If LDAP is disabled, this setting disables standard Web browser (RFC2617) authentication/login and forces the use of the https login screen.

Directory Service Access Configuration

LDAP Auth UserName: LDAPuserName
LDAP Auth Password: ••••••••••••••••••••
Confirm Password:

Directory Service Email Alert Configuration

LDAP Email Alert Enable: □
LDAP Alert Table Refresh: 0 Hours

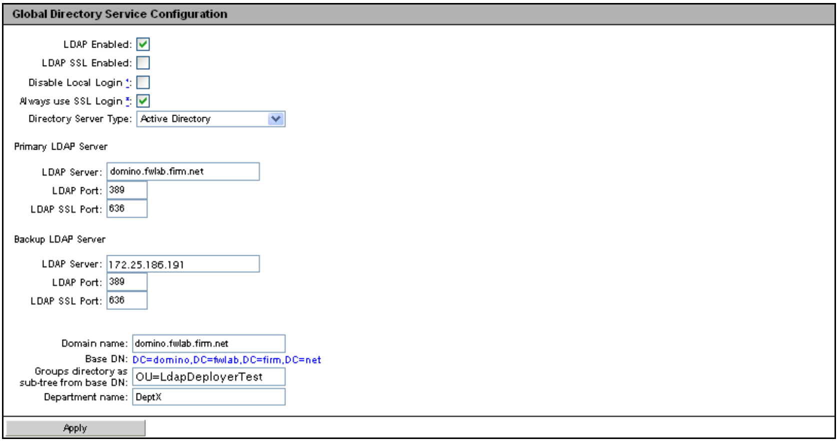
© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.
19-Jan-2011 22:09:23

Figure 158: Directory Service Configuration: Specifications for Microsoft Active Directory

The entries shown as examples in figure 158 refer to the examples and figures shown in the "User Management in ServerView" manual.

Proceed as follows:

► Complete your specifications in the *Global Directory Service Configuration* group:



Global Directory Service Configuration

LDAP Enabled: ☑
LDAP SSL Enabled: □
Disable Local Login *: □
Always use SSL Login *: ☑
Directory Server Type: Active Directory

Primary LDAP Server

LDAP Server: domino.fwlab.firm.net
LDAP Port: 389
LDAP SSL Port: 636

Backup LDAP Server

LDAP Server: 172.25.186.191
LDAP Port: 389
LDAP SSL Port: 636

Domain name: domino.fwlab.firm.net
Base DN: DC=domino,DC=fwlab,DC=firm,DC=net
Groups directory as sub-tree from base DN: OU=LdapDeployerTest
Department name: DeptX

Figure 159: Global Directory Service Configuration: Specifications for Microsoft Active Directory

Primary LDAP Server

LDAP directory server that is to be used.

LDAP Server

IP address or DSN name of the primary LDAP server.

LDAP Port

LDAP port of the primary LDAP server.

LDAP SSL Port

Secure LDAP port of the primary LDAP server

Backup LDAP Server

LDAP directory server which is maintained as the backup server and used as the directory server if *LDAP Server 1* fails.

LDAP Server

IP address or DSN name of the Backup LDAP server.

LDAP Port

LDAP port of the Backup LDAP server.

LDAP SSL Port

Secure LDAP port of the Backup LDAP server

Domain Name

Complete DNS path name of the directory server.

Base DN

Base DN is automatically derived from *Domain Name*.

Groups directory as sub-tree from base DN

Pathname of the organizational unit (OU) which as a subtree of *Base DN* (Group DN Context) contains the OUs *SVS* or *iRMCgroups*.

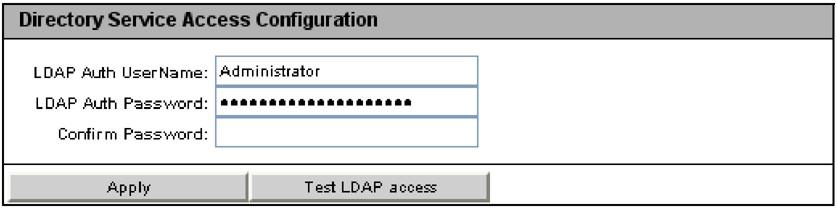
Department name

The department name is used in the directory service in order to determine the user permissions and alert roles. A user may have different permissions for the department X server than for the department Y server.

- Click *Apply* to activate your settings.

- Configure the LDAP access data in the *Directory Service Access Configuration* group:

i The settings that you make here are required for alerting in connection with global user identifications. If alerting is not enabled, the settings in the *Directory Service Access Configuration* group are not significant.


Directory Service Access Configuration

LDAP Auth UserName: Administrator

LDAP Auth Password: ●●●●●●●●●●●●●●●●●●●●

Confirm Password:

Figure 160: Microsoft Active Directory: Directory Service Access Configuration

LDAP Auth User Name

User name the iRMC S2/S3 uses to log onto the LDAP server.

LDAP Auth Password

Password the user specified under User Name uses to authenticate themselves on the LDAP server.

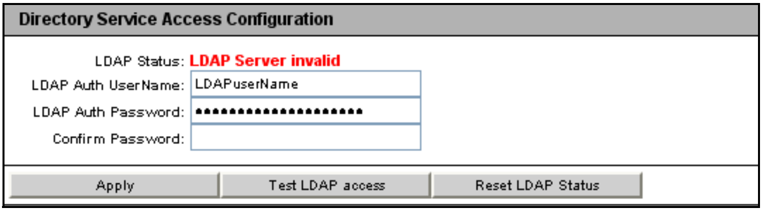
Confirm Password

Repeat the password you entered under *LDAP Auth Password*.

Test LDAP Access

Checks the access data to the LDAP directory server and shows the LDAP status as the result (see figure 161).

> i This test only checks the basic access data (“Is the LDAP server present?”, “Is the user configured?”), but does not fully authenticate the user.



Directory Service Access Configuration

LDAP Status: LDAP Server invalid

LDAP Auth UserName: LDAPuserName

LDAP Auth Password: ••••••••••••••••••••

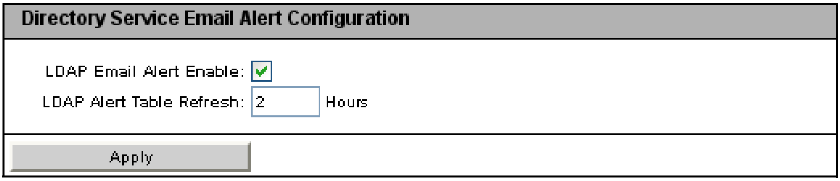
Confirm Password:

Figure 161: Microsoft Active Directory: Status of the connection to the LDAP server

- Click *Reset LDAP Status* to reset the status display.

- Click *Apply* to activate your settings.

- Configure the settings for global email alerting in the *Directory Service Email Alert Configuration* group.



Directory Service Email Alert Configuration

LDAP Email Alert Enable: ☑

LDAP Alert Table Refresh: 2 Hours

Figure 162: Directory Service Email Alert Configuration

LDAP Email Alert Enable

Enables global email alerting.

LDAP Alert Table Refresh [Hours]

Defines the interval at which the email table is regularly updated (see the "User Management in ServerView" manual).

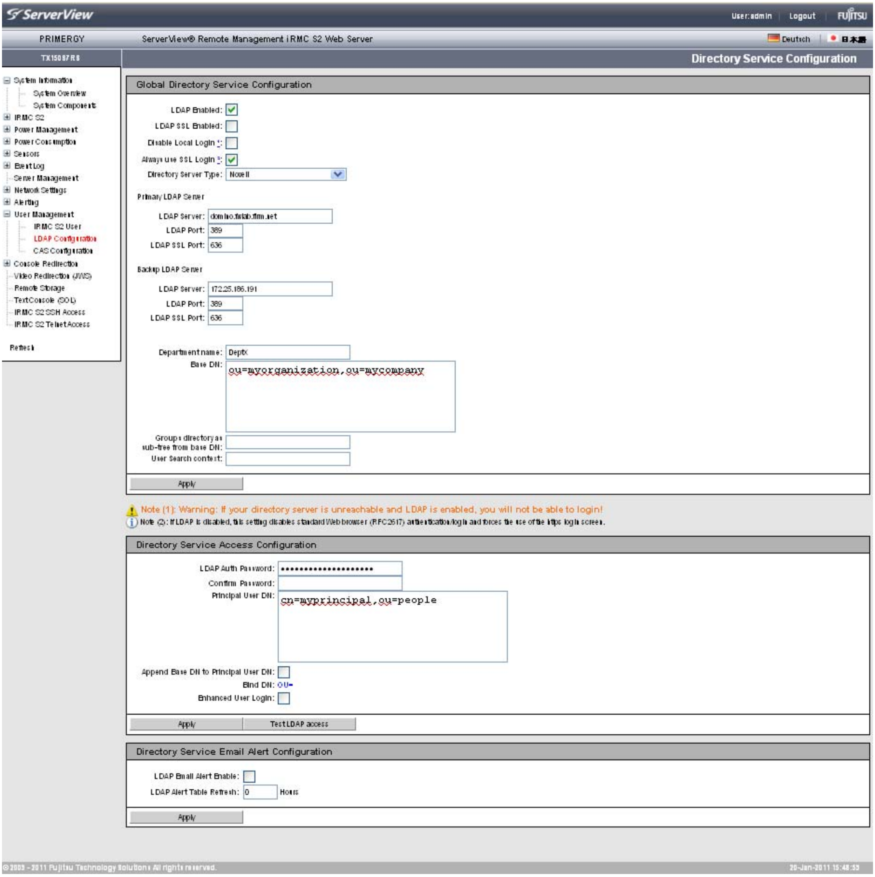
> i It is strongly recommended that you specify a value >0. A value of “0” means that the table is not updated regularly.

- Click *Apply* to activate your settings.

7.14.2.2 Configuring iRMC S2/S3 for Novell eDirectory / OpenLDAP / OpenDS

After you have confirmed you choice of *Novell* or *OpenLDAP* by clicking *Apply*, the following variant of the *Directory Service Configuration* page is shown.

> The *Directory Service Configuration* page has an identical structure for Novell eDirectory, OpenLDAP and OpenDS.



Directory Service Configuration

Global Directory Service Configuration

LDAP Enabled: ☑
LDAP SSL Enabled: □
Disable Local Login ¹: □
Always use SSL Login ²: ☑
Directory Server Type: Novell

Primary LDAP Server

LDAP Server: domino.fwlab.firm.net
LDAP Port: 389
LDAP SSL Port: 636

Backup LDAP Server

LDAP Server: 172.25.186.191
LDAP Port: 389
LDAP SSL Port: 636

Department name: DeptX
Base DN: ou=myorganization,ou=mycompany
Groups directory as sub-tree from base DN:
User Search context:

Note (1): Warning: If your directory server is unreachable and LDAP is enabled, you will not be able to login!
Note (2): If LDAP is disabled, this setting disables standard Web browser (RFC2617) authentication/login and forces the use of the https login screen.

Directory Service Access Configuration

LDAP Auth Password: ••••••••••••••••••••
Confirm Password:
Principal User DN: cn=myprincipal,ou=people
Append Base DN to Principal User DN: □
Bind DN: ou=
Enhanced User Login: □

Directory Service Email Alert Configuration

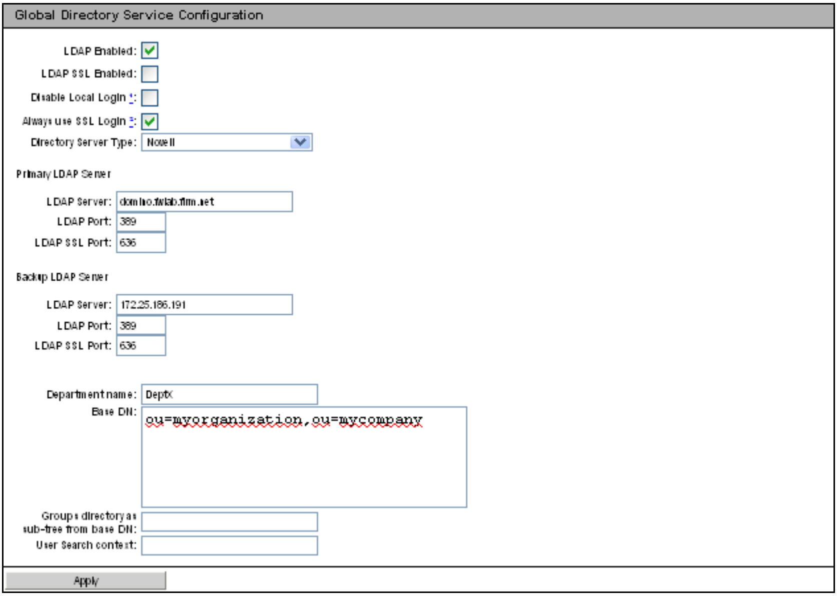
LDAP Email Alert Enable: □
LDAP Alert Table Refresh: 0 Hours

Figure 163: Global Directory Service Configuration: Specifications for Novell eDirectory / Open LDAP

> The entries shown as examples in figure 163 refer to the examples and figures shown in the "User Management in ServerView" manual.

Proceed as follows:

► Complete your specifications in the *Global Directory Service Configuration* group:



Global Directory Service Configuration

LDAP Enabled: ☑

LDAP SSL Enabled: □

Disable Local Login *: □

Always use SSL Login *: ☑

Directory Server Type: Novell

Primary LDAP Server

LDAP Server: domino.fwlab.firm.net

LDAP Port: 389

LDAP SSL Port: 636

Backup LDAP Server

LDAP Server: 172.25.186.191

LDAP Port: 389

LDAP SSL Port: 636

Department name: DeptX

Base DN: ou=myorganization,ou=mycompany

Groups directory as sub-tree from base DN:

User Search context:

Figure 164: Global Directory Service Configuration: Specifications for Novell eDirectory / Open LDAP / OpenDS

Primary LDAP Server

LDAP directory server that is to be used.

LDAP Server

IP address or DSN name of the primary LDAP server.

LDAP Port

LDAP port of the primary LDAP server.

LDAP SSL Port

Secure LDAP port of the primary LDAP server

Backup LDAP Server

LDAP directory server which is maintained as the backup server and used as the directory server if *LDAP Server 1* fails.

LDAP Server

IP address or DSN name of the Backup LDAP server.

LDAP Port

LDAP port of the Backup LDAP server.

LDAP SSL Port

Secure LDAP port of the Backup LDAP server

Department Name

Department name. The directory service needs the department name in order to determine the user permissions. A user may have different permissions for the department X server than for the department Y server.

Base DN

The *Base DN* is the fully distinguished name of the eDirectory or Open LDAP server and represents the tree or subtree that contains the OU (Organizational Unit) *SVS* or *iRMCgroups*. This DN forms the starting point for LDAP searches.

Groups directory as sub-tree from base DN

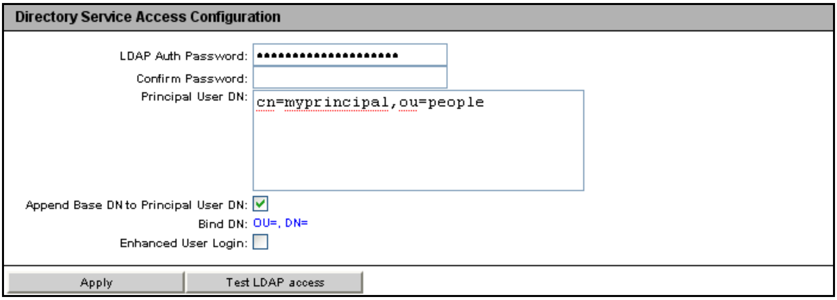
Pathname of the OU which as a subtree of *Base DN* (Group DN Context) contains the OUs *SVS* or *iRMCgroups*.

User Search Context

Pathname of the OU which as a subtree of *Base DN* (User Search Context) contains the OU unit *Users*.

► Click *Apply* to activate your settings.

► Configure the LDAP access data in the *Directory Service Access Configuration* group:



Directory Service Access Configuration

LDAP Auth Password: ••••••••••••••••••••

Confirm Password:

Principal User DN: cn=myprincipal,ou=people

Append Base DN to Principal User DN: ☑

Bind DN: OU=, DN=

Enhanced User Login: □

Figure 165: Novell eDirectory / Open LDAP: Directory Service Access Configuration

LDAP Auth Password

Password the *Principal User* uses to authenticate themselves on the LDAP server.

Confirm Password

Repeat the password you entered under *LDAP Auth Password*.

Principal User DN

Fully distinguished name, i.e. the full description of the object path and attributes of the generic iRMC S2/S3 user ID (principal user), under which the iRMC S2/S3 queries the permissions of the iRMC S2/S3 users from the LDAP server.

Append Base DN to Principal User DN

If you activate this option, you do not need to specify the Base DN under *Principal User DN*. In this event, the Base DN is used that you specified under *Base DN* in the *Global Directory Service Configuration* group.

Bind DN

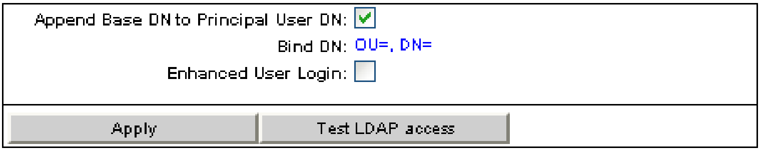
Bind DN shows the principal user DN used for LDAP authentication.

Enhanced User Login

Enhanced flexibility when users log in.

CAUTION!

Only activate this option if you are familiar with the LDAP syntax. If you inadvertently specify and activate an invalid search filter, users can only log in to the iRMC S2/S3 under a global login after the *Enhanced User Login* option has been deactivated.



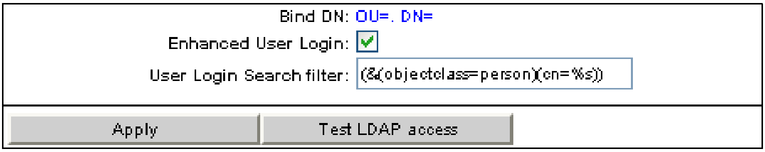
Append Base DN to Principal User DN: ☑

Bind DN: OU=, DN=

Enhanced User Login: □

Figure 166: Enhanced User Login

If you select *Enhanced User Login* and activate it with *Apply*, an additional field *User Login Search Filter* appears containing the standard login search filter "(&(objectclass=person)(cn=%s))".



Bind DN: OU=, DN=

Enhanced User Login: ☑

User Login Search filter: (&(objectclass=person)(cn=%s))

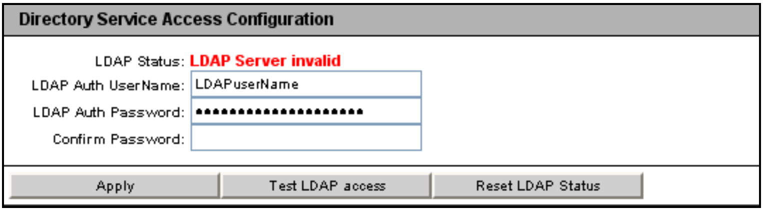
Figure 167: LDAP search filter for “Enhanced User Login”

At login, the placeholder “%s” is replaced by the associated global login. You can modify the standard filter by specifying another attribute in place of “cn=”. All global logins are then permitted to log into the iRMC S2/S3 which meet the criteria of this search filter.

Test LDAP Access

Checks the access data to the LDAP directory server and shows the LDAP status as the result (see figure 161).

i This test only checks the basic access data (“Is the LDAP server present?”, “Is the user configured?”), but does not fully authenticate the user.



Directory Service Access Configuration

LDAP Status: LDAP Server invalid

LDAP Auth UserName: LDAPuserName

LDAP Auth Password: ********************

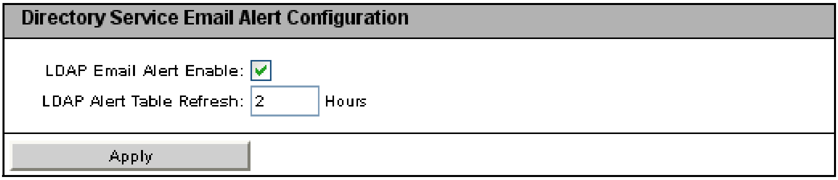
Confirm Password:

Figure 168: eDirectory / OpenLDAP: Status of the connection to the LDAP server

- Click *Reset LDAP Status* to reset the status display.

- Click *Apply* to activate your settings.

- Configure the settings for global email alerting in the *Directory Service Email Alert Configuration* group.



Directory Service Email Alert Configuration

LDAP Email Alert Enable: ☑

LDAP Alert Table Refresh: 2 Hours

Figure 169: Directory Service Email Alert Configuration

LDAP Email Alert Enable

Enables global email alerting.

LDAP Alert Table Refresh [Hours]

Defines the interval at which the email table is regularly updated (see the "User Management in ServerView" manual). A value of “0” means that the table is not updated regularly.

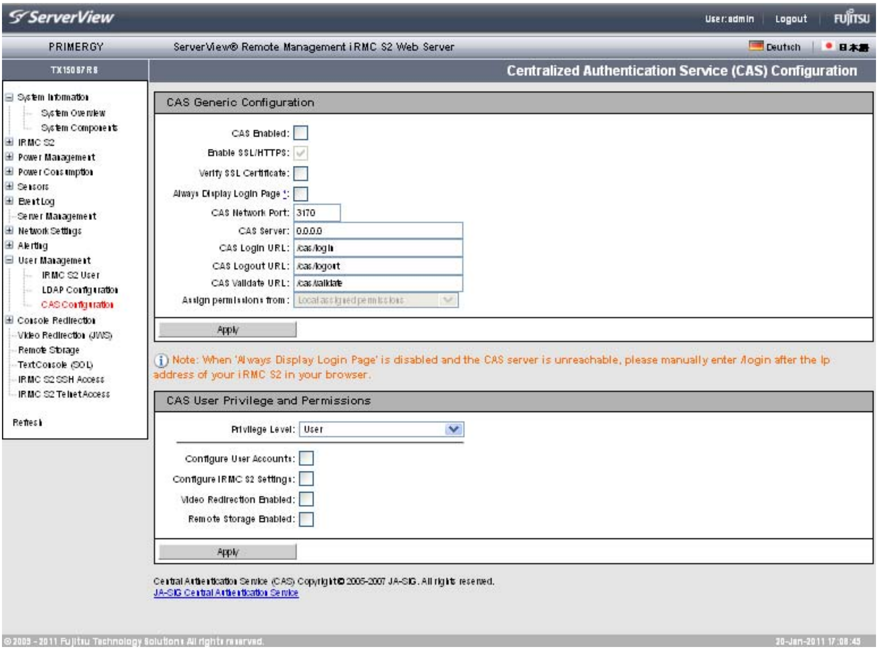
- Click *Apply* to activate your settings.

7.14.3 Centralized Authentication Service (CAS) Configuration - Configuring the CAS Service

> This view is not supported by all PRIMERGY servers with iRMC S2/S3.
>
> SSO is only supported for accessing the iRMC S2/S3 via the web interface. SSO is **not** supported for accessing the iRMC S2/S3 via the Remote Manager (Telnet/SSH).

The *Centralized Authentication Service (CAS) Configuration* page allows you to configure the iRMC S2/S3 web interface for CAS-based single sign-on (SSO) authentication.

The first time a user logs in to an application within the SSO domain of the CAS service, they are prompted for their credentials by the CAS-specific login screen. Once they have been successfully authenticated by the CAS service, the user is granted access to the iRMC S2/S3 web interface as well as to any other service within the SSO domain without being prompted for login credentials again.



CAS Generic Configuration

CAS Enabled: □
Enable SSL/HTTPS: ☑
Verify SSL Certificate: □
Always Display Login Page *: □
CAS Network Port: 3170
CAS Server: 0.0.0.0
CAS Login URL: /cas/login
CAS Logout URL: /cas/logout
CAS Validate URL: /cas/validate
Assign permissions from: Local assigned permissions

Note: When 'Always Display Login Page' is disabled and the CAS server is unreachable, please manually enter /login after the Ip address of your iRMC S2 in your browser.

CAS User Privilege and Permissions

Privilege Level: User
Configure User Accounts: □
Configure iRMC S2 Settings: □
Video Redirection Enabled: □
Remote Storage Enabled: □

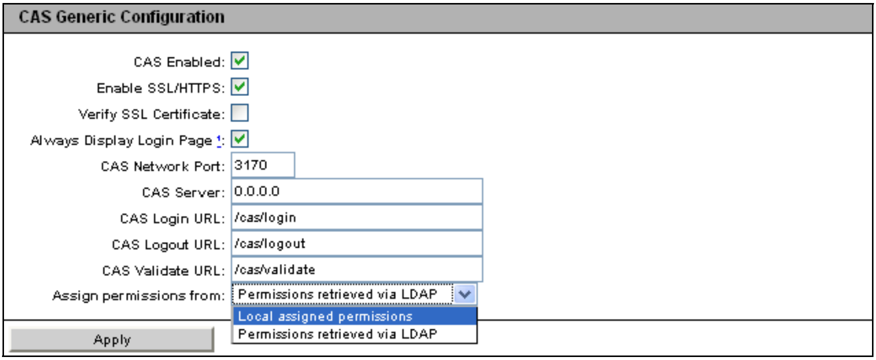
Central Authentication Service (CAS) Copyright© 2005-2007 JA-SIG. All rights reserved.
JA-SIG Central Authentication Service

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.
20-Jan-2011 17:08:45

Figure 170: Centralized Authentication Service (CAS) Configuration

CAS Generic Configuration

The *CAS Generic Configuration* group allows you to configure CAS access data.



CAS Generic Configuration

CAS Enabled: ☑

Enable SSL/HTTPS: ☑

Verify SSL Certificate: □

Always Display Login Page ¹: ☑

CAS Network Port: 3170

CAS Server: 0.0.0.0

CAS Login URL: /cas/login

CAS Logout URL: /cas/logout

CAS Validate URL: /cas/validate

Assign permissions from: Permissions retrieved via LDAP

Figure 171: CAS Generic Configuration

CAS Enabled

Enables SSO using the CAS service that you specify in the *CAS Generic Configuration* group.

Enable SSL/HTTPS

All communication between the CAS service and the iRMC S2/S3 is SSL encrypted.

Verify SSL Certifikate

The SSL Certificate of the CAS service is checked against the CA Certificate.

Always Display Login Page

If *Always Display Login Page* is disabled and the CAS service cannot be reached, type `/login` after the IP address of the iRMC S2/S3 in your browser’s navigation bar.

Always displays the iRMC S2/S3 login page:

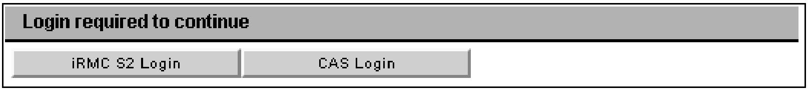
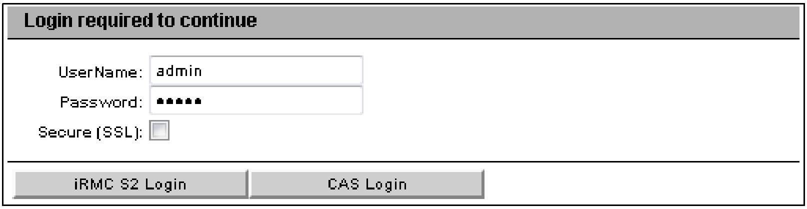


Figure 172: Login page



UserName: admin
Password: •••••
Secure (SSL): □

Figure 173: Login page - explicit authentication required

This allows users to temporarily login at the iRMC S2/S3 with privileges and permissions that differ from the authorization profile defined under *CAS User Privilege and Permissions* (see page 290).

A user may, for instance, currently be logged in to the CAS service under a user ID with the *User* privilege and now wants to perform an action requiring the *Administrator* privilege. The user can temporarily login at the iRMC S2/S3 under a user ID with the required privileges. However, the user cannot switch between both user IDs.

The buttons *iRMC Login* and *CAS Login* work as follows:

iRMC S2/S3 Login

Logs the user in to the iRMC S2/S3 web interface with the values specified for *User name* and *Password.* The CAS service is bypassed.

CAS Login

Logs the user in to the iRMC S2/S3 web interface via SSO:

- If the user has not been authenticated by the CAS service yet: The user is redirected to the CAS service for authentication with the specified values for *User name* and *Password*.
- If the user has already been authenticated by the CAS service: The user is logged in at the iRMC S2/S3 without being prompted for username and password.

CAS Network Port

Port of the CAS service.
Default port number: 3170

CAS Server

DNS name of the CAS service.

i It is absolutely necessary that all systems participating in the SSO domain reference the Central Management Station (CMS) via the same addressing representation. (An SSO Domain comprises all systems where authentication is performed using the same CAS service.) Thus, for example, if you have installed the ServerView Operations Manager by using the name "my-cms.my-domain", you must specify exactly the same name for configuring the CAS service for an iRMC S2/S3. If, instead, you specify only "my-cms" or another IP address of my-cms, SSO will not be enabled between the two systems.

CAS LoginURL

Login URL of the CAS service.

CAS Logout URL

Logout URL of the CAS service.

CAS Validate URL

Validate URL of the CAS service.

Assign permissions from

Defines the iRMC S2/S3 privilege and permissions for users who are logged in to the iRMC S2/S3 via SSO:

Local assigned permissions

The privilege and permissions defined under *CAS User Privileg and Permissions* apply to the user.

Permissions retrieved via LDAP

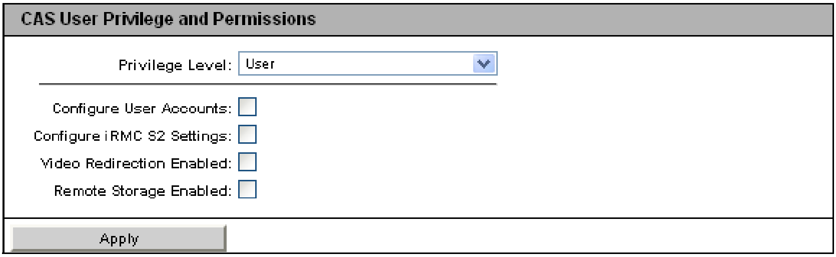
The authorization profile defined in the LDAP directory service applies to the user.

The *Permissions retrieved via LDAP* option is only available, if LDAP is enabled (see option "LDAP Enabled" on page 274).

CAS User Privilege and Permissions

The *CAS User Privilege and Permissions* group allows you to define the iRMC S2/S3 privilege and permissions a user is granted if they are logged in at the iRMC S2/S3 via SSO.

The *CAS User Privilege and Permissions* group is not displayed if you have selected *Permissions retrieved via LDAP* under *Permissions assigned from* in the *CAS Generic Configuration* group.



CAS User Privilege and Permissions

Privilege Level: User

Configure User Accounts: □

Configure iRMC S2 Settings: □

Video Redirection Enabled: □

Remote Storage Enabled: □

Figure 174: CAS User Privilege and Permissions

Privilege

Assign a privilege group to the user here:

- *User*
- *Operator*
- *Administrator*
- *OEM*

Refer to section "User permissions" on page 68 for information on the permissions associated with the privilege groups.

In addition to the IPMI specific permissions, you can also individually assign users the following channel-independent permissions:

Configure User Accounts

Permission to configure local user access data.

Configure iRMC S2/S3 Settings

Permission to configure the iRMC S2/S3 settings.

Video Redirection enabled

Permission to use Advanced Video Redirection (AVR) in “View Only” and “Full Control” mode.

Remote Storage enabled

Permission to use the Remote Storage functionality.

7.15 Console Redirection - Redirecting the console

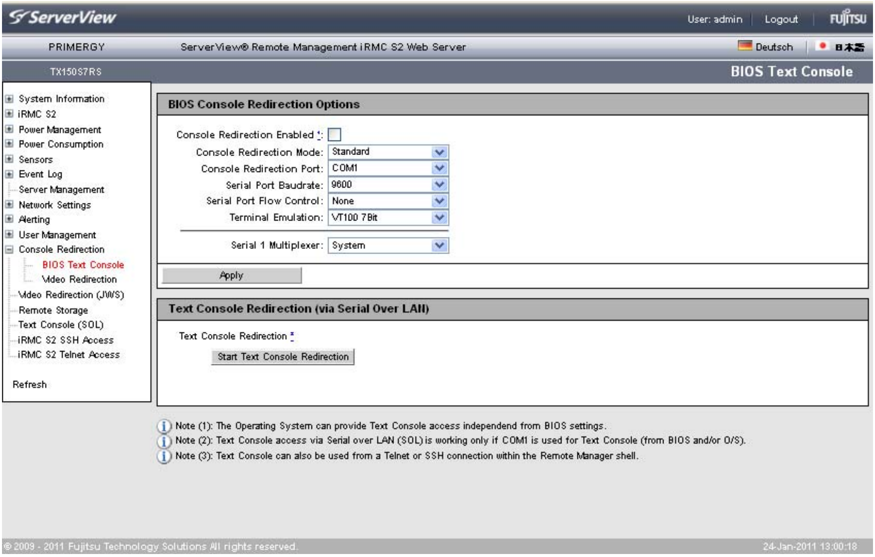
The following pages are available for console redirection:

- "BIOS Text Console - Configure and start text console redirection" on page 292.
- "Advanced Video Redirection - Start Advanced Video Redirection (AVR)" on page 302.

7.15.1 BIOS Text Console - Configure and start text console redirection

The *BIOS Text Console* page allows you to configure and start text console redirection.

Text console redirection can also be configured in the BIOS (see section "Configuring text console redirection for the iRMC S3" on page 53).



BIOS Console Redirection Options

Console Redirection Enabled ¹: □
Console Redirection Mode: Standard
Console Redirection Port: COM1
Serial Port Baudrate: 9600
Serial Port Flow Control: None
Terminal Emulation: VT100 7Bit
Serial 1 Multiplexer: System

Apply

Text Console Redirection (via Serial Over LAN)

Text Console Redirection ²

Start Text Console Redirection

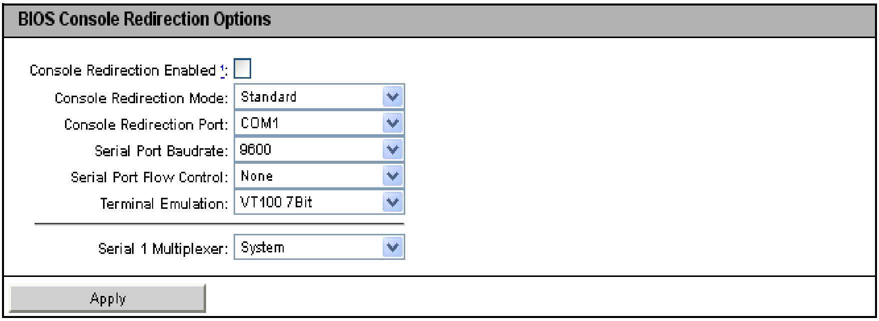
Note (1): The Operating System can provide Text Console access independend from BIOS settings.
Note (2): Text Console access via Serial over LAN (SOL) is working only if COM1 is used for Text Console (from BIOS and/or O/S).
Note (3): Text Console can also be used from a Telnet or SSH connection within the Remote Manager shell.

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.
24-Jan-2011 13:00:18

Figure 175: BIOS Text Console page

7.15.1.1 BIOS Console Redirection Options - Configure text console redirection

BIOS Console Redirection Options allows you to configure text console redirection.



BIOS Console Redirection Options

Console Redirection Enabled 1: □
Console Redirection Mode: Standard
Console Redirection Port: COM1
Serial Port Baudrate: 9600
Serial Port Flow Control: None
Terminal Emulation: VT100 7Bit

Serial 1 Multiplexer: System

Figure 176: BIOS Text Console page - BIOS Console Redirection Options

Console Redirection Enabled

This option allows you to enable / disable console redirection.

> i The operating system can also permit text console redirection irrespective of the settings in the BIOS.

Console Redirection Mode

This setting affects the behavior of console redirection while the operating system is running (after the BIOS POST phase has completed) - see section "Text console redirection while the operating system is running" on page 300:

Standard

Console redirection is terminated after the BIOS POST phase.

Enhanced

Console redirection continues to be available after the BIOS POST phase.

Console Redirection Port

Two serial ports are available: *Serial 1*, *Serial 2*.

i If console redirection is to be performed via LAN, Serial 1 must be set.

If *Serial 2* is selected, only the connection over the null modem cable works.

Serial Port Baud Rate

The following baud rates can be set: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Serial Port Flow Control

The following settings are possible:

None

Flow control is disabled.

XON/XOFF (Software)

Flow control is handled by the software.

CTS/RTS (Hardware)

Flow control is handled by the hardware.

Terminal Emulation

The following terminal emulations are available:

VT100 7Bit, VT100 8Bit, *PC-ANSI 7Bit*, *PC-ANSI 8 Bit, VT100+*, *VT-UTF8*

Serial 1 Multiplexer

Check the consistency of the multiplexer settings:

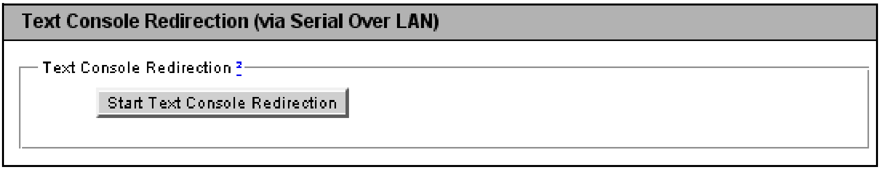
- Serial: System
- LAN: iRMC S2/S3

► Click *Apply* to activate your settings.

7.15.1.2 Text Console Redirection (via Serial over LAN) - Start text console redirection

Text Console Redirection (via Serial Over LAN) allows you to start text console redirection.

i Text console redirection via Serial over LAN (SOL) assumes that the operating system and / or the BIOS use serial port 1 (COM1) for text console redirection.



Text Console Redirection (via Serial Over LAN)
Text Console Redirection ?
Start Text Console Redirection

Figure 177: Start text console redirection via Serial over LAN (SOL).

► Click *Start Console Redirection* to start text console redirection function.

The Java applet for text console redirection is started (see figure 178 on page 296):

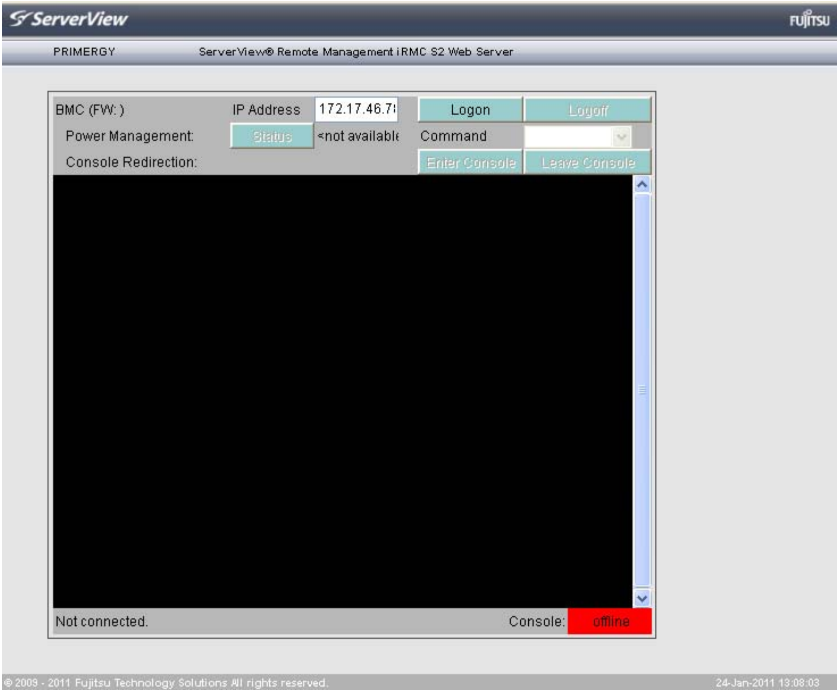
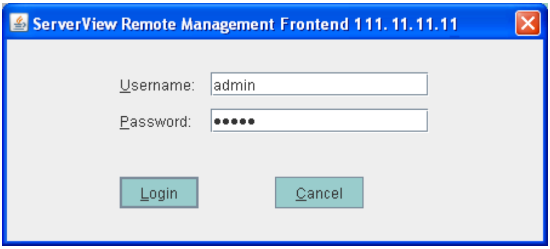


Figure 178: Window for power management and text console redirection (before login)

► Click *Logon* to log in to the iRMC S2/S3.

You are then prompted to enter your iRMC S2/S3 user name and password:



Username: admin

Password: •••••

Figure 179: Power management and text console redirection - Login window

► Enter your user name and password and click *Login* to confirm.

The window for power management and text console redirection is then displayed:

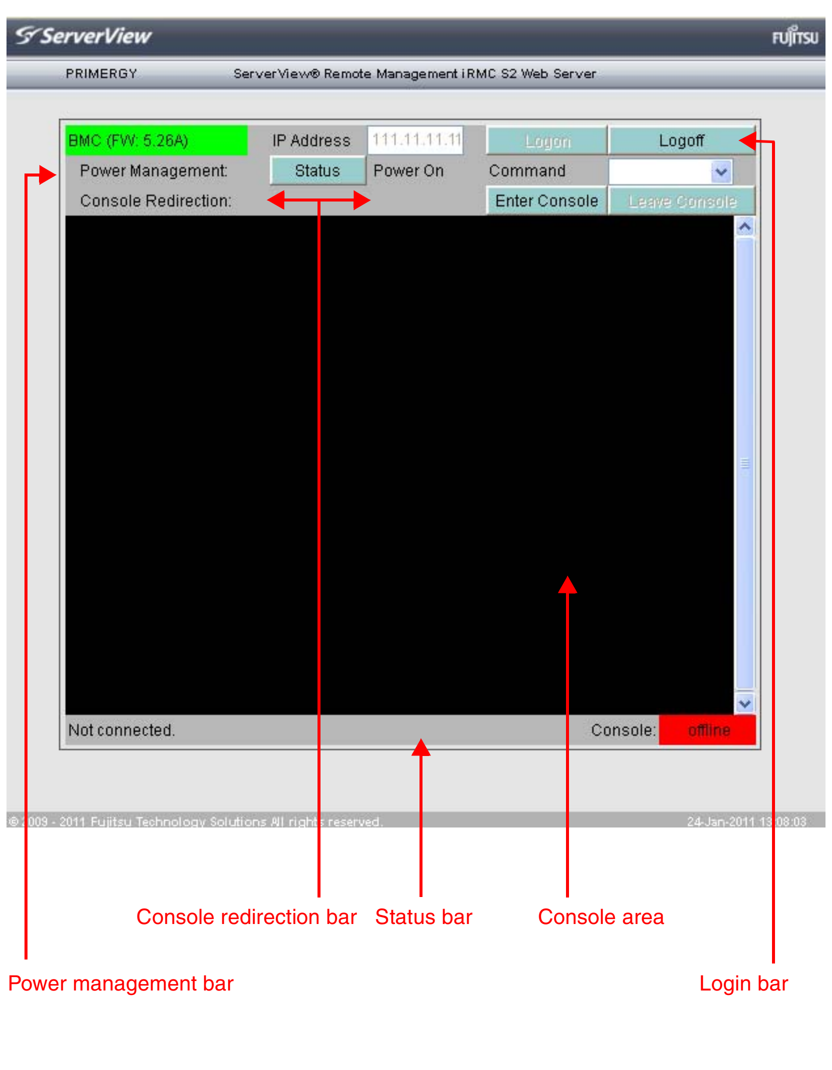


Figure 180: Window for power management and text console redirection

The elements of the console redirection window are explained below:

Login bar

The login bar shows the IP address and current firmware version of the iRMC S2/S3. The *Login* and *Logout* buttons allow you to log in to and log out of the iRMC S2/S3.

Power management bar

The power management bar provides information on the power status of the managed server. You can update the display by clicking the *Status* button.

The *Command* drop-down list allows you to select and launch an IPMI command for power management of the managed server (see page page 299). You do not need to be connected with the console to do this.

Console redirection bar

The *Enter Console* and *Leave Console* buttons in the console redirection bar allow you to show or hide the display in the console area.

Console area

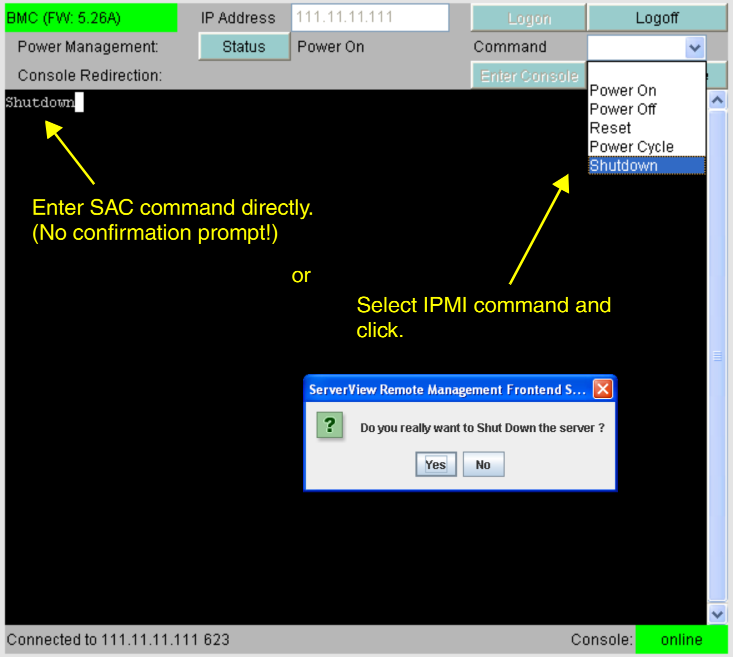
The console area contains the display from the redirected text console.

Status bar

The status bar shows the IP address of the iRMC S2/S3 and the port number used for console redirection. In addition, the status bar provides information on the status of the console redirection (online / offline).

► Click *Enter Console*.

You are then connected to the console and can execute the required command, either by entering it directly in the console area or by clicking it in the *Command* drop-down list (IPMI commands only):



```
Shutdown
```

Do you really want to Shut Down the server ?

Figure 181: Entering SAC or IPMI commands at the console.

IPMI command	Explanation
Power On	Switches the server on.
Power Off	Switches the server off.
Reset	Completely restarts the server (cold start), regardless of the status of the operating system.
Power Cycle	Powers the server down completely and then powers it up again after approximately 5 seconds.
Shutdown	Graceful shutdown and power off.

► To close the connection to the console, click *Leave Console*.

7.15.1.3 Text console redirection while the operating system is running

Depending on the operating system used on the managed server, you can continue to use console redirection after the BIOS / UEFI POST phase.

DOS

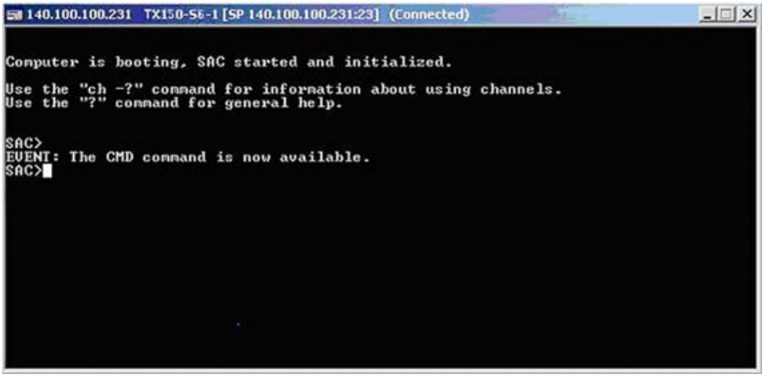
Condition:

The BIOS setting for console redirection mode must be set to *Enhanced* (see the section "BIOS Text Console - Configure and start text console redirection" on page 292).

If the managed server starts the PRIMERGY ServerView Suite diagnosis software, you can operate PRIMERGY ServerView Suite diagnosis using console redirection.

Windows Server 2003 / 2008

Windows Server 2003 / 2008 handles console redirection automatically after the POST phase. No further settings are necessary. While the operating system is booting, the Windows Server 2003 SAC console / Windows Server 2008 SAC console is transferred:



140.100.100.231 TX150-S6-1 [SP 140.100.100.231:23] (Connected)

```
Computer is booting, SAC started and initialized.

Use the "ch -?" command for information about using channels.
Use the "?" command for general help.


SAC>
EVENT: The CMD command is now available.
SAC>
```

Figure 182: Windows Server 2003 SAC console

Linux

You must configure a Linux operating system in such a way that it handles console redirection after the POST phase. Once it has been configured, you have complete remote access.

Settings required

The settings may differ between program versions.

SuSe and RedHat

Add the following line to the end of the file */etc/inittab*:

```
xx:12345:respawn:/sbin/agetty <baud-rate> ttyS0
```

RedHat

Insert the following kernel boot parameter in the file */etc/grub.conf*:

```
console=ttyS0,<baud-rate> console=tty0
```

SuSE

Insert the following kernel boot parameter in the file */boot/grub/menu.lst*:

```
console=ttyS0,<baud-rate> console=tty0
```

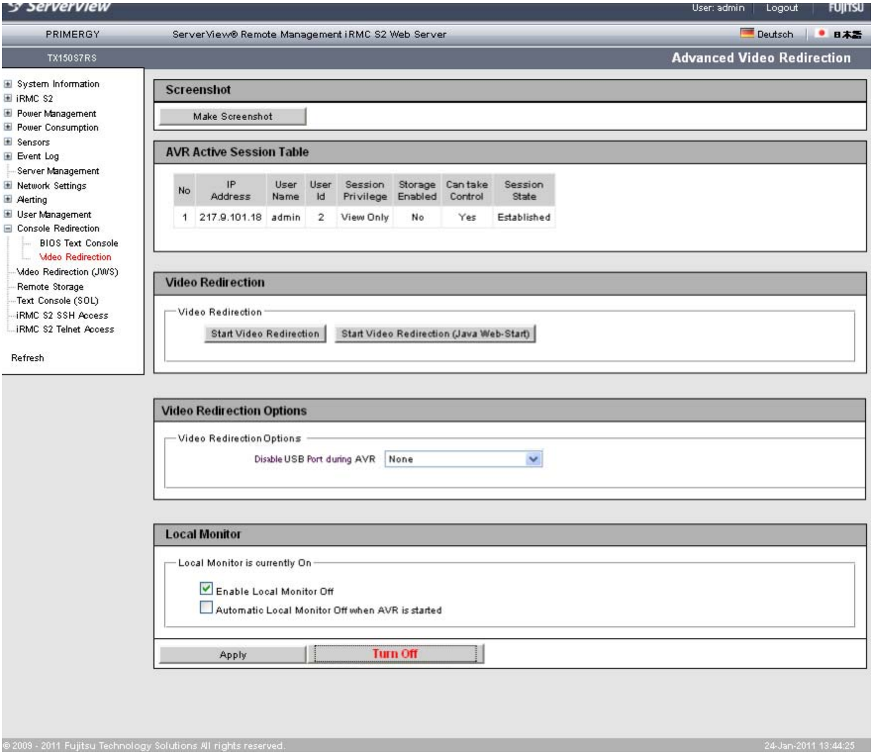
7.15.2 Advanced Video Redirection - Start Advanced Video Redirection (AVR)

The *Advanced Video Redirection* page allows you to start graphical console redirection. The “Advanced Video Redirection” feature redirects graphical output from the managed server to the remote workstation and assigns keyboard and mouse input from the remote workstation to the managed server so that you can access the managed server from the remote workstation as if you were working locally.

AVR can be used by two users simultaneously. One user has full control over the server (full-control mode) and the other can only passively observe keyboard and mouse operation of the server (view-only mode).

ℹ In order to use the iRMC S2/S3 function *Advanced Video Redirection*, you require a license key (see section "iRMC S2/S3 Information - Information on the iRMC S2/S3" on page 165).

The AVR functionality is made available with a Java applet.



AVR Active Session Table

No	IP Address	User Name	User Id	Session Privilege	Storage Enabled	Can take Control	Session State
1	217.9.101.18	admin	2	View Only	No	Yes	Established

Video Redirection Options

Disable USB Port during AVR: None

Local Monitor

Local Monitor is currently On

☑ Enable Local Monitor Off

□ Automatic Local Monitor Off when AVR is started

Figure 183: Advanced Video Redirection page

Creating an ASR screenshot

The *ASR Screenshot* page allows you to

- take a screenshot of the current VGA screen on the managed server (video screenshot) and store it in the firmware of the iRMC S2/S3,
- view the screenshot stored in the iRMC S2/S3 firmware,
- delete the screenshot stored in the iRMC S2/S3 firmware,

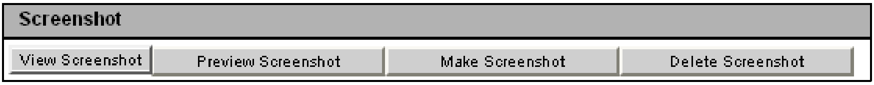


Figure 184: Creating an video screenshot

A video screenshot is automatically created on ASR&R events - in Windows, these are typically watchdog events or "bluescreens" on the managed server.

A maximum of **one** video screenshot is stored in the firmware of the iRMC S2/S3, namely the most recently created screenshot.

The following actions are available by clicking on one of the buttons displayed:

View Screenshot
(This only appears if a video screenshot has been stored.)
The screenshot is shown in a separate browser window.

Preview Screenshot
(This only appears if a video screenshot has been stored.)
A thumbnail of the screenshot is shown in the *ASR Screenshot* group.

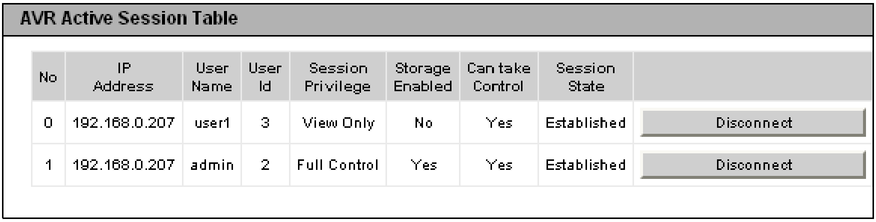
Make Screenshot
Takes a new video screenshot.

Delete Screenshot
(This only appears if a video screenshot has been stored.)
The video screenshot stored in the iRMC S2/S3 firmware is deleted after you have confirmed that you wish to do so.

AVR Active Session Table - Show current AVR sessions

The *AVR Active Session Table* lists the currently active AVR sessions. If no AVR session is currently active then the *AVR Active Session Table* is not displayed.

If two AVR Sessions are currently active, a *Disconnect* button is displayed for each Session.



AVR Active Session Table

No	IP Address	User Name	User Id	Session Privilege	Storage Enabled	Can take Control	Session State	
0	192.168.0.207	user1	3	View Only	No	Yes	Established	Disconnect
1	192.168.0.207	admin	2	Full Control	Yes	Yes	Established	Disconnect

Figure 185: AVR Active Session Table - (two active AVR sessions)

Disconnect

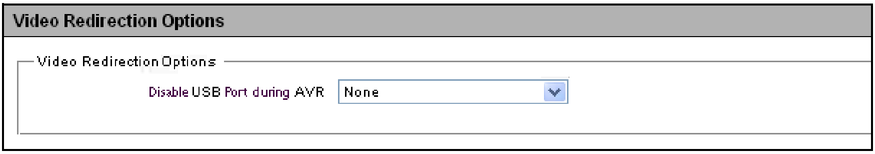
If you click *Disconnect*, a confirmation dialog box appears in which you can close the AVR session to the left of the button.

> i You can only close AVR sessions of other users with the *Disconnect* button. To close your own session, choose *Exit* from the *Extras* menu in the AVR window (see page 102).

Video Redirection Options - Deactivating USB ports on the managed server for the duration of the AVR session

> i This function is not supported for all PRIMERGY servers.

Video Redirection Options - Disable USB Port allows you to specify which USB ports are to be disabled on the managed server for the duration of the AVR session.



Video Redirection Options

Video Redirection Options

Disable USB Port during AVR: None

Figure 186: Video Redirection Options

None

No USB port will be disabled.

Front USB

Only the USB port on the front of the server will be disabled.

Rear USB

Only the USB port on the back of the server will be disabled.

Disable All

All USB ports of the server will be disabled.

► Click *Apply* to activate your settings.

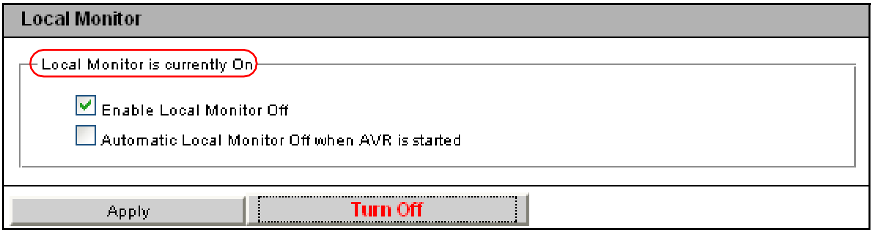
Local Monitor - Power up / down options for local server monitor

The status of the local monitor on the managed server is shown under *Local Monitor* (see section "Local Monitor Off" function" on page 90).

In addition, you can configure:

– that the local monitor can be switched on and off from the remote workstation,

– that the local monitor shuts down automatically for the duration of the AVR session when an AVR session is started,



Local Monitor

Local Monitor is currently On

☑ Enable Local Monitor Off

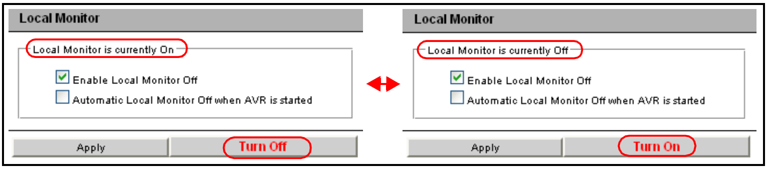
☐ Automatic Local Monitor Off when AVR is started

Figure 187: Advanced Video Redirection page - Local Monitor

Enable Local Monitor Off

This option allows you to activate the following options:

- In full-control mode of an AVR session, you can switch the local monitor on and off (AVR *Extras* menu, see page 102).
- For **users with administrator or OEM permissions**, the toggle button *Turn Off* / *Turn On* is also enabled. This also allows the local monitor to be switched on and off (see figure 188).



Local Monitor

Local Monitor is currently On

☑ Enable Local Monitor Off

□ Automatic Local Monitor Off when AVR is started

Apply | Turn Off

Local Monitor

Local Monitor is currently Off

☑ Enable Local Monitor Off

□ Automatic Local Monitor Off when AVR is started

Apply | Turn On

Figure 188: Advanced Video Redirection page - Local Monitor On / Off

- You can also configure that the local monitor is switched off automatically for the duration of an AVR session when an AVR session is started (see the *Automatic Local Monitor Off when AVR is started* option).

i If no concurrent session with Local Monitor Off is active, the local monitor is automatically switched on again when the AVR session is closed.

Automatic Local Monitor Off when AVR is started

i This option only takes effect if *Enable Local Monitor* has been activated.

If you activate this option, the local monitor is automatically switched off for the duration of the session when an AVR session is started. After the AVR session is closed, the local monitor is automatically switched on again if no concurrent session with Local Monitor Off is active.

i **Parallel AVR sessions:**

Even if you switch on the local monitor during your AVR session (in the AVR menu *Extras* or with the *Turn On* button), the local monitor is automatically switched off again if a new, concurrent AVR session is started.
The local monitor is switched on again automatically when all AVR sessions have been closed.

► Click *Apply* to activate your settings.

Video Redirection - Starting AVR

You start AVR under *Video Redirection*.

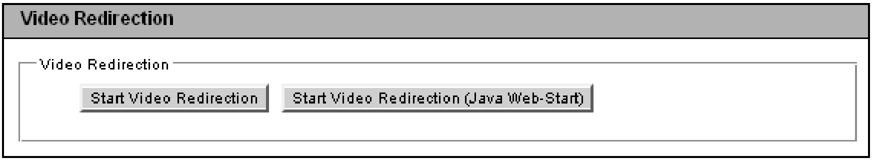
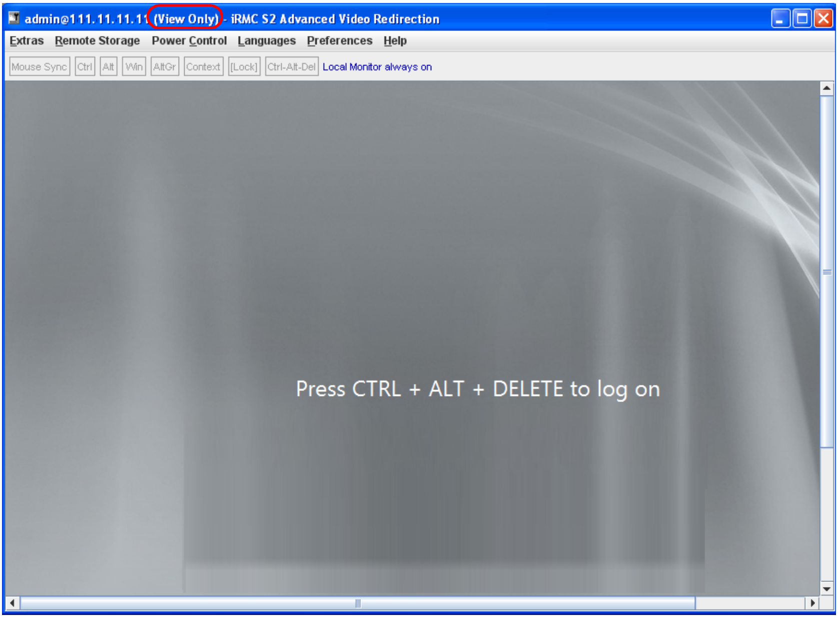


Figure 189: Advanced Video Redirection page - Local Monitor

► Click *Start Video Redirection* or *Start Video Redirection (Java Web-Start)* to start a second AVR session.

The Java applet for Advanced Video Redirection is started.

> The Java applet shows the AVR window in view-only mode if another user already uses AVR in full-control mode. Otherwise, the Java applet shows the AVR window in full-control mode.



Press CTRL + ALT + DELETE to log on

Figure 190: AVR window (view-only mode)

► Select *Extras - Take Full Control...* in the AVR menu (see page 103 for details), to take over full control of the managed server.

> i If you attempt to take full control of the managed server using AVR, an already existing full-control session will be notified. by the following dialog:
>
> If the full-control session refuses your attempt to take full control, your session will remain in view-only mode. Users should agree among themselves what modes they are to use in their sessions.

If you succeeded in taking full control, the window for active use of AVR is opened, with which you can log into the managed server (see figure 191 on page 309).

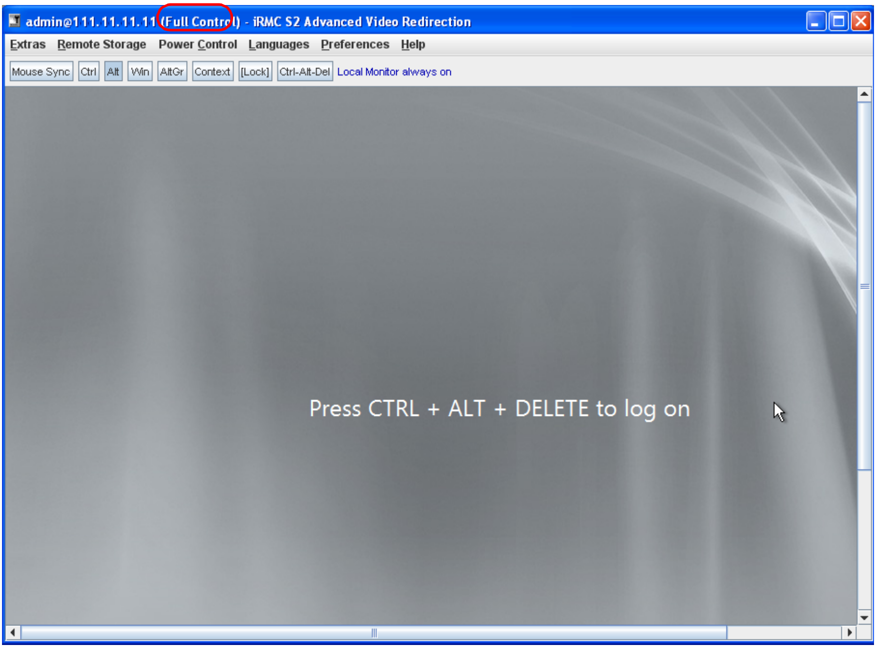
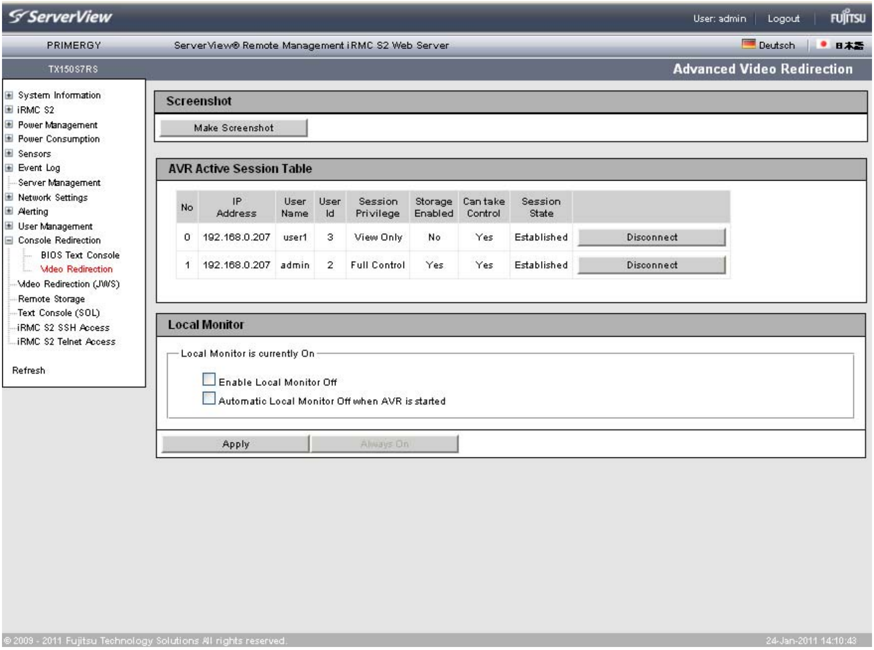

admin@111.11.11.11 (Full Control) - iRMC S2 Advanced Video Redirection
Extras Remote Storage Power Control Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del Local Monitor always on
Press CTRL + ALT + DELETE to log on

Figure 191: AVR window (full-control mode)

The menus of the AVR window and the integrated special keys are described in chapter "Advanced Video Redirection (AVR)" on page 85.

The two active AVR sessions are shown as follows on the *Advanced Video Redirection* page:



AVR Active Session Table

No	IP Address	User Name	User Id	Session Privilege	Storage Enabled	Can take Control	Session State	
0	192.168.0.207	user1	3	View Only	No	Yes	Established	Disconnect
1	192.168.0.207	admin	2	Full Control	Yes	Yes	Established	Disconnect

Local Monitor

Local Monitor is currently On

□ Enable Local Monitor Off
□ Automatic Local Monitor Off when AVR is started

Figure 192: AVR window with two active AVR sessions

Disconnect

If you click *Disconnect*, a confirmation dialog box appears in which you can close the AVR session to the left of the button.

i You can only close AVR sessions of other users with the *Disconnect* button. To close your own session, choose *Exit* from the *Extras* menu in the AVR window (see page 102).

The following window appears if the managed server is powered down:

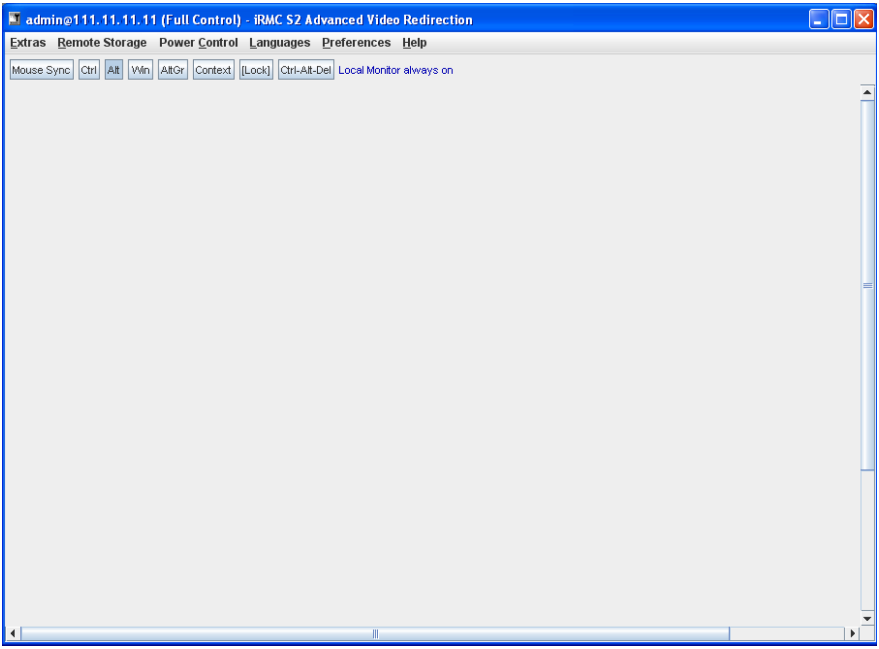


Figure 193: AVR window when the server is powered down

7.16 Remote Storage

The Remote Storage feature provides the managed server with a “virtual” drive which is physically located elsewhere in the network. The source for the virtual drive can be a physical drive (floppy disk drive CD-ROM/DVD-ROM) or an ISO image (image file).

i In order to use the iRMC S2/S3 function *Remote Storage*, you require a license key (see page 167).

You can make the remote storage media available as follows:

- As a physical drive or image file at the remote workstation (see page 113). The image file may also be a network drive (with drive letter, e.g. “D:” for drive D).
- As an image file centrally in the network via a remote storage server (see page 127).

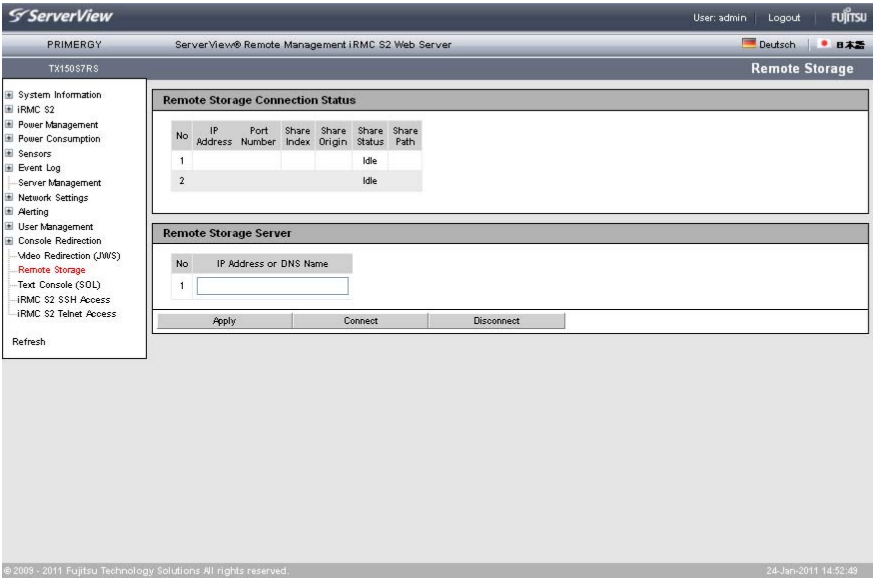
i **Parallel remote storage connections:**

The following are possible concurrently:

- **either up to two** Remote Storage connections to virtual drives at the remote workstation (if the connection is established over the AVR Java applet) **or**
- **one** Remote Storage connection to a Remote Storage server.

Remote storage connections via applet and Remote Storage Server are not possible simultaneously.

The *Remote Storage* page allows you to display information on the status of the current remote storage connections and establish the connection to a remote storage server.



Remote Storage Connection Status

No	IP Address	Port Number	Share Index	Share Origin	Share Status	Share Path
1					Idle	
2					Idle	

Remote Storage Server

No	IP Address or DNS Name
1	

Figure 194: Remote Storage page

Remote Storage Connection Status

Displays the status of the remote storage connection:

No

Displays the sequential number of the remote storage device.

IP Address

Displays the IP address of the server or workstation on which the remote storage device is installed.

Share Index

Displays the number assigned to the remote storage connection.

Share Origin

Displays the status of the remote storage device on a server or on a remote workstation:

- *Applet*: Connectable
- *None*: Not connectable (Not found)

Share Status

Displays the current status of the connection:

- *Connected*: Connected
- *Idle*: Not connected

Remote Storage Server

Allows you to specify a computer on which a remote storage server is installed.

No

Displays the sequential number of the remote storage server.

IP Address or DNS Name

Specifies the IP address or the registered DNS name of the computer on which a remote storage server is installed.

Apply

Click *Apply* to save the remote storage server’s IP address or DNS name.

Connect

Click *Apply* to save the remote storage server’s IP address or DNS name and establish the connection to the remote storage server.

i Before it is possible to establish the connection to the remote storage server the remote storage server must be installed and running.

Disconnect

Click *Disconnect* to terminate the connection to the remote storage server.

7.17 Operating iRMC S2/S3 via Telnet / SSH (Remote Manager)

A Telnet / SSH-based interface is available for the iRMC S2/S3. This is known as the Remote Manager. The alphanumeric user interface of the Remote Manager provides you with access to system and sensor information, power management functions and the error event log. You can also start text console redirection and a SMASH CLP shell.

You can call the Remote Manager from the iRMC S2/S3 web interface as follows:

- Use the *iRMC S2/S3 SSH Access* link to initiate an SSH (**S**ecure **Sh**ell) encrypted Telnet connection to the iRMC S2/S3.
- Use the *iRMC S2/S3 Telnet Access* link to initiate an unencrypted Telnet connection to the iRMC S2/S3.

Calling the Remote Manager from the iRMC S2/S3 web interface automatically starts a Java applet, which implements a Telnet / SSH client. Telnet / SSH access to Remote Manager using the Java applet is provided for convenience (e.g. no SSH client is supplied together with Windows operating systems). However, to access the Remote Manager, you can use any Telnet or SSH Client.

ℹ If you establish an SSH connection using the Java applet, public key authentication is not supported.

ℹ Maximum number of parallel sessions:

- Telnet: up to 4
- SSH: up to 4
- Telnet and SSH in total: up to 4

Operation of the iRMC S2/S3 using the Remote Manager is described in chapter "iRMC S2/S3 via Telnet/SSH (Remote Manager)" on page 321.

Requirements on the managed server

Access via Telnet must be activated for the iRMC S2/S3 (see the section "Ports and Network Services - Configuring ports and network services" on page 245).

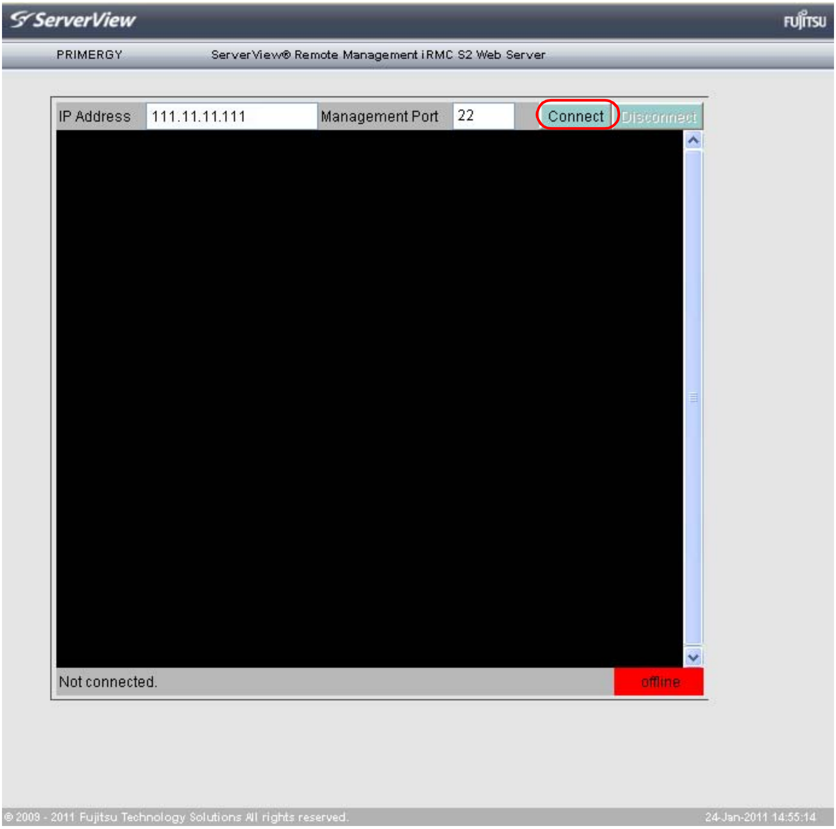
ℹ Access via the Telnet protocol is deactivated by default for security reasons, as passwords are transmitted in plain text.

Establishing an SSH / Telnet connection and logging into the Remote Manager

> **i** If the screen displays for SSH and Telnet connections differ only with respect to the connection-specific information displayed, the display for an SSH connection is shown below.

► In the navigation bar, click on the link *iRMC S2/S3 SSH Access* (SSH) or *iRMC S2/S3 Telnet Access* (Telnet).

The Java applet for the SSH or Telnet connection is started and the following window is displayed (in this case using the example of an SSH connection):



IP Address 111.11.11.111 Management Port 22

Not connected.

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved. 24-Jan-2011 14:55:14

Figure 195: Establishing an SSH connection to the iRMC S2/S3

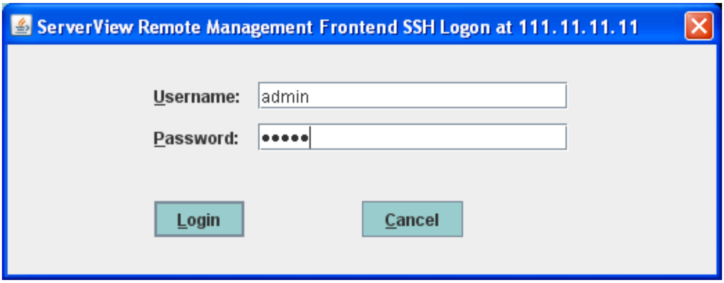
► In the connection bar, click *Connect*.

As soon as the connection to the iRMC S2/S3 has been established, you are requested to enter the user name and password.

– *Logging into the Remote Manager over an SSH connection*

ℹ If the host key of the managed server is not yet registered at the remote workstation, the SSH client issues a security alert with suggestions on how to proceed.

The following login window is displayed:



ServerView Remote Management Frontend SSH Logon at 111.11.11.11

Username: admin

Password: •••••

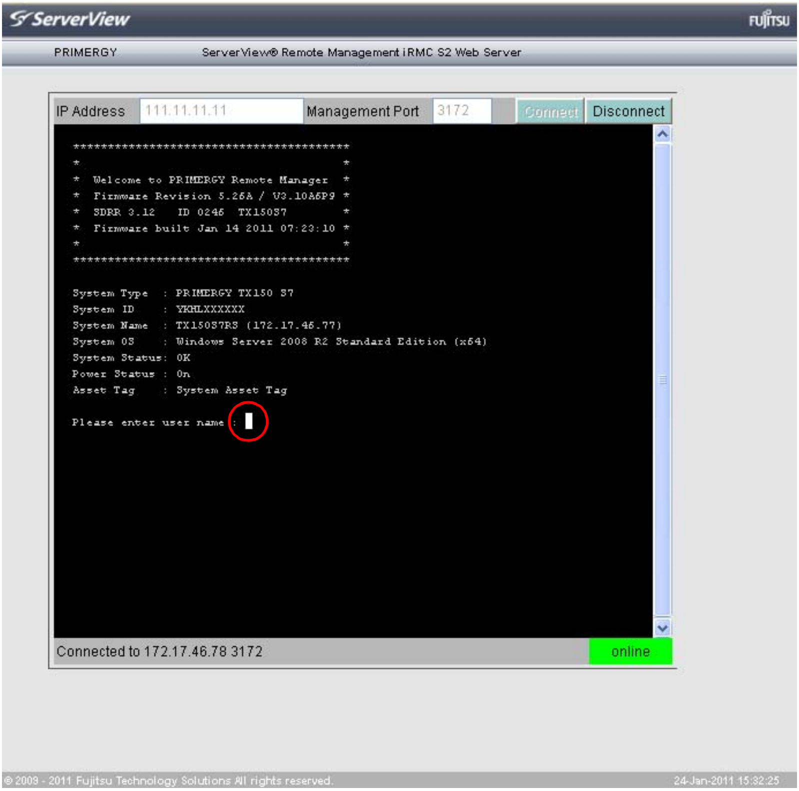
Figure 196: SSH connection: Logging in to the Remote Manager

► Enter your user name and password and confirm your entries by clicking *Login*.

The main menu of the Remote Manager is then displayed (see figure 198 on page 319).

– *Logging into the Remote Manager over a Telnet connection*

The Remote Manager login window is displayed:



IP Address 111.11.11.11 Management Port 3172

```
****************************************
*                                      *
*  Welcome to PRIMERGY Remote Manager  *
*  Firmware Revision 5.26A / V3.10A6P9 *
*  SDRR 3.12   ID 0246  TX150S7        *
*  Firmware built Jan 14 2011 07:23:10 *
*                                      *
****************************************

System Type   : PRIMERGY TX150 S7
System ID     : YKHLXXXXXX
System Name   : TX150S7RS (172.17.46.77)
System OS     : Windows Server 2008 R2 Standard Edition (x64)
System Status: OK
Power Status : On
Asset Tag     : System Asset Tag

Please enter user name :
```

Connected to 172.17.46.78 3172

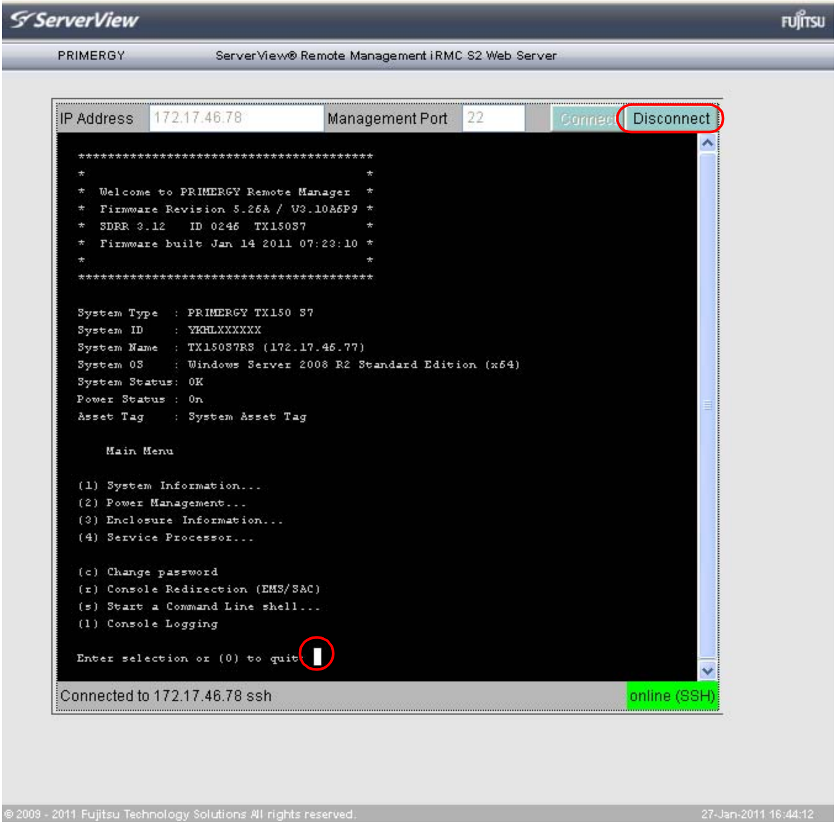
© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.   24-Jan-2011 15:32:25

Figure 197: Telnet connection: Logging in to the Remote Manager

i Depending on whether ServerView agents have already been started at some point on the system, the login window is shown with or without system information (see page 326).

► Enter your user name and password and confirm your entries by pressing [Enter].

The main menu of the Remote Manager is then displayed (see figure 198 on page 319).



```
  ****************************************
  *                                      *
  *  Welcome to PRIMERGY Remote Manager  *
  *  Firmware Revision 5.26A / V3.10A6P9 *
  *  SDRR 3.12    ID 0246  TX150S7       *
  *  Firmware built Jan 14 2011 07:23:10 *
  *                                      *
  ****************************************

  System Type   : PRIMERGY TX150 S7
  System ID     : YKHLXXXXXX
  System Name   : TX150S7RS (172.17.46.77)
  System OS     : Windows Server 2008 R2 Standard Edition (x64)
  System Status: OK
  Power Status  : On
  Asset Tag     : System Asset Tag

      Main Menu

  (1) System Information...
  (2) Power Management...
  (3) Enclosure Information...
  (4) Service Processor...

  (c) Change password
  (r) Console Redirection (EMS/SAC)
  (s) Start a Command Line shell...
  (l) Console Logging

  Enter selection or (0) to quit:
```

Connected to 172.17.46.78 ssh

online (SSH)

© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.
27-Jan-2011 16:44:12

Figure 198: Main menu of the Remote Manager

Closing a Telnet / SSH connection

► Close the connection to the Remote Manager by clicking the *Disconnect* button in the connection bar of the Remote Manager window or by pressing the [0] key in the main menu of the Remote Manager (see figure 198).

8 iRMC S2/S3 via Telnet/SSH (Remote Manager)

A Telnet-based interface is available for the iRMC S2/S3. This is known as the Remote Manager. You can call the Remote Manager over the following interfaces:

– iRMC S2/S3 web interface (see page 315)
– any Telnet/SSH client

The iRMC S2/S3 supports secure connections over SSH (**S**ecure **Sh**ell). The Remote Manager interface is identical for Telnet and SSH connections. In principle, any Telnet/SSH client that interprets VT100 sequences can be used to access the iRMC S2/S3. It is nevertheless recommended that the iRMC S2/S3 web interface or the ServerView Remote Management Frontend (referred to below simply as the Remote Management Frontend) be used.

ℹ Maximum number of parallel sessions:

– Telnet: up to 4
– SSH: up to 4
– Telnet and SSH in total: up to 4

This chapter describes operation of the iRMC S2/S3 from the Remote Manager and the various functions in detail. The end of the chapter also provides a brief overview of SMASH CLP.

8.1 Requirements on the managed server

Access via Telnet must be activated for the iRMC S2/S3 (see the section "Ports and Network Services - Configuring ports and network services" on page 245).

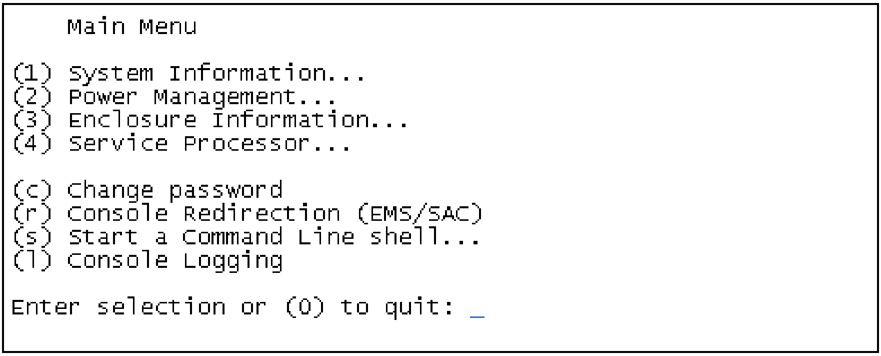
ℹ Access via the Telnet protocol is deactivated by default for security reasons, as passwords are transmitted in plain text.

ℹ Since the ServerView Operations Manager does not know the value of the management port, the Remote Management Frontend works with the default value.

Since a connection is not automatically established when the Remote Management Frontend is started, you can correct any nonstandard value for the management port after the Remote Management Frontend has been started.

8.2 Operating Remote Manager

Operation of Remote view is described on the basis of the example in figure 199, which shows an excerpt from the main menu of the Remote Manager.



```
    Main Menu

(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...

(c) Change password
(r) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
(l) Console Logging

Enter selection or (0) to quit: _
```

Figure 199: Operating the Remote Manager

- ▸ Select the required menu item by entering the number or letter which precedes the menu item, e.g. “c” for “Change password”.

  Functions that the user is not permitted to use are indicated by a dash (-) and functions that are not available are indicated by an asterisk (*).

- ▸ Press 0 or the key combination Ctrl D to close the Remote Manager. An appropriate event will be written to the event log.

8.3 Overview of menus

The Remote Manager menu for the iRMC S2/S3 has the following structure:

- **System Information**
  - View Chassis Information
  - View Mainboard Information
  - View OS and SNMP Information
  - Set ASSET Tag
- **Power Management**
  - Immediate Power Off
  - Immediate Reset
  - Power Cycle
  - Power on
  - Graceful Power Off (Shutdown)
  - Graceful Reset (Reboot)
  - Raise NMI (via iRMC S2/S3)
- **Enclosure Information**
  - System Eventlog
    - View System Eventlog (text, newest first)
    - View System Eventlog (text, oldest first)
    - Dump System Eventlog (raw, newest first)
    - Dump System Eventlog (raw, oldest first)
    - View System Eventlog Information
    - Clear System Eventlog

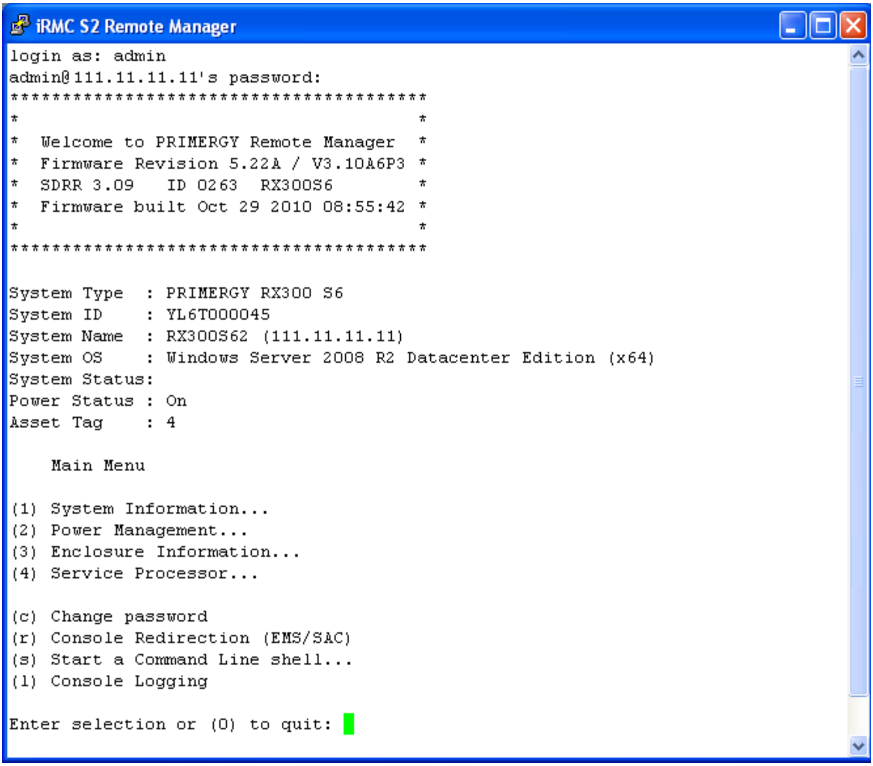
  - Internal Eventlog
    - View Internal Eventlog (text, newest last)
    - Dump Internal Eventlog (raw, newest last)
    - View Internal Eventlog Information
    - Clear Internal Eventlog
    - Change Internal Eventlog mode
  - Temperature
  - Voltages/Current
  - Fans
  - Power Supplies
  - Memory Sensor
  - Door Lock
  - CPU Sensors
  - Component Status (Lightpath)
  - List All Sensors
- **Service Processor**
  - Configure IP Parameters
  - List IP Parameters
  - Toggle Identify LED
  - Reset iRMC S2/S3 (Warm reset)
  - Reset iRMC S2/S3 (Cold reset)
- **Change password**
- **Console Redirection (EMS/SAC)**
- **Start a Command Line shell**
- **Console Logging**

8.4 Logging in

When connecting to the iRMC S2/S3, you are required to enter your login credentials (username and password). As soon as a connection to the iRMC S2/S3 has been established, the main menu window of the Remote Manager (Telnet/SSH window) is displayed at the terminal client at the remote workstation.

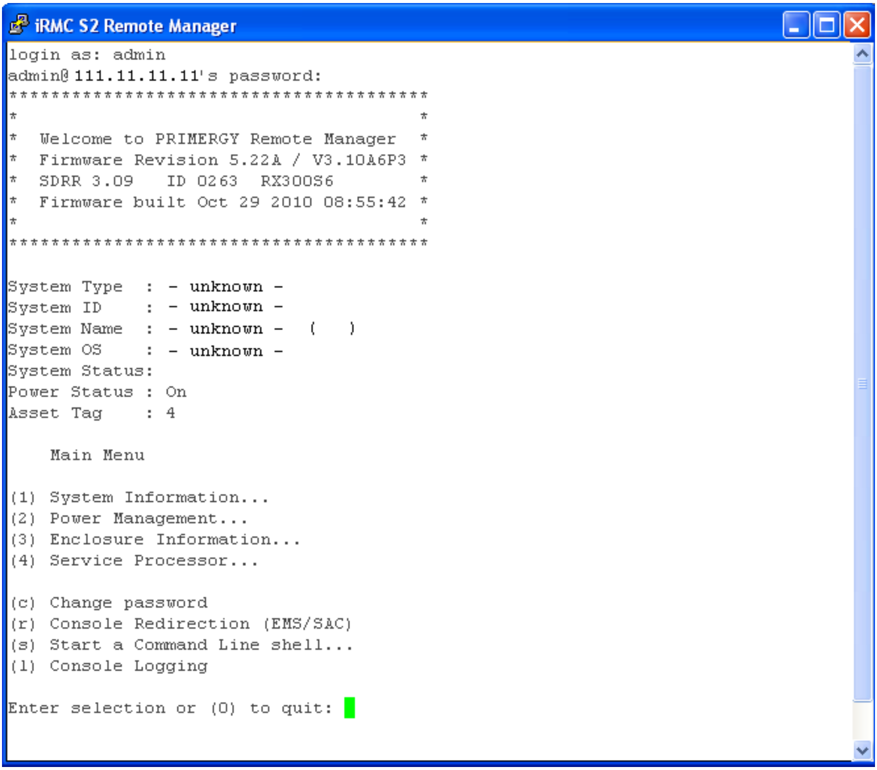
Depending on whether ServerView agents have already been started at some point on the system, the main window is shown with or without system information.

When logging in over an SSH connection: If the host key of the managed server is not yet registered at the remote workstation, the SSH client issues a security alert with suggestions on how to proceed.



```
login as: admin
admin@111.11.11.11's password:
****************************************
*                                      *
*  Welcome to PRIMERGY Remote Manager  *
*  Firmware Revision 5.22A / V3.10A6P3 *
*  SDRR 3.09    ID 0263   RX300S6      *
*  Firmware built Oct 29 2010 08:55:42 *
*                                      *
****************************************

System Type   : PRIMERGY RX300 S6
System ID     : YL6T000045
System Name   : RX300S62 (111.11.11.11)
System OS     : Windows Server 2008 R2 Datacenter Edition (x64)
System Status:
Power Status  : On
Asset Tag     : 4

    Main Menu

(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...

(c) Change password
(r) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
(l) Console Logging

Enter selection or (0) to quit:
```

Figure 200: Remote Manager: Main menu window (with system information)



```
login as: admin
admin@111.11.11.11's password:
***************************************
*                                     *
*  Welcome to PRIMERGY Remote Manager  *
*  Firmware Revision 5.22A / V3.10A6P3 *
*  SDRR 3.09    ID 0263   RX300S6      *
*  Firmware built Oct 29 2010 08:55:42 *
*                                     *
***************************************

System Type   :  - unknown -
System ID     :  - unknown -
System Name   :  - unknown -   (   )
System OS     :  - unknown -
System Status:
Power Status  : On
Asset Tag     : 4

    Main Menu

(1)  System Information...
(2)  Power Management...
(3)  Enclosure Information...
(4)  Service Processor...

(c)  Change password
(r)  Console Redirection (EMS/SAC)
(s)  Start a Command Line shell...
(l)  Console Logging

Enter selection or (0) to quit:
```

Figure 201: Remote Manager: Main menu window (without system information)

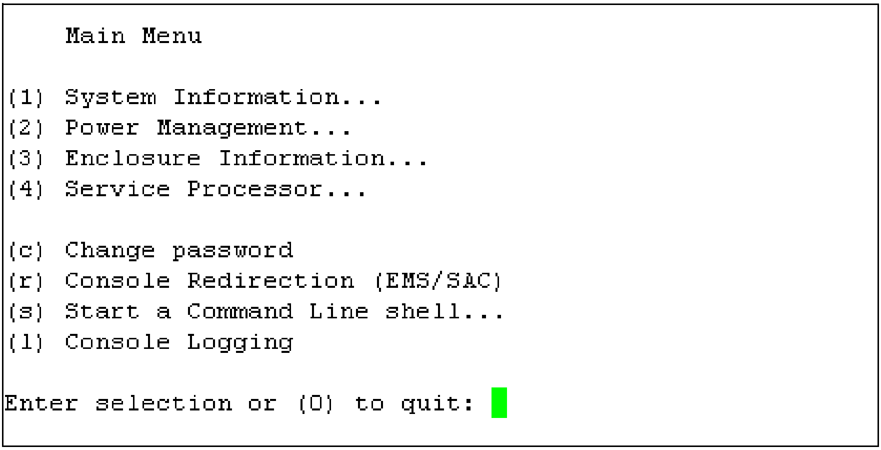
The Remote Manager window contains information on the affected system. This information identifies the server and indicates its operating status (Power Status). Some details (e.g. the System Name) are only shown for servers and only if the server is configured appropriately.

► In order to be able to use the Remote Manager, you must log in with a user name and a password.

  Then an appropriate event will be written to the Event log and the relevant main menu of the Remote Manager displayed (see section "Main menu of the Remote Manager" on page 328).

  You can terminate the login process at any time using [Ctrl] [D].

8.5 Main menu of the Remote Manager



```
    Main Menu

(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...

(c) Change password
(r) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
(l) Console Logging

Enter selection or (0) to quit:
```

Figure 202: Remote Manager: Main menu

The main menu of the Remote Manager provides the following functions:

System Information...	View information on the managed server and set the Asset Tag (see section "System Information - Information on the managed server" on page 332).
Power Management...	Power the server up or down. (see section "Power Management" on page 334).
Enclosure Information...	Request information on the current system status, e.g. check error and event messages from the error log and event log (temperature, fan, etc.) (see section "Enclosure Information - System event log and status of the sensors" on page 335).

Table 8: Main menu of the Remote Manager

Service Processor...	Configure the iRMC S2/S3iRMC S2/S3 (e.g. update firmware or change IP address) (see section "Service processor - IP parameters, identification LED and iRMC S2/S3 reset" on page 339).
Change password	Change the password (see section "Change the password" on page 332).
Console Redirection (EMS/SAC)	Text console redirection (see section "Console Redirection (EMS/SAC) - Start text console redirection" on page 340).
Start a Command Line shell...	Start a command line shell (see section "Start a Command Line shell... - Start a SMASH CLP shell" on page 340).
Console Logging	Redirect output of messages to the text console (see section "Console Logging - Redirect message output to the text console (serial)" on page 341).

Table 8: Main menu of the Remote Manager

8.6 Required user permissions

In table 9 is given an overview of the user permissions which are required in order to use the individual Remote Manager functions.

Remote Manager menu items	Permitted with IPMI privilege level				Required permission			
	OEM	Administrator	Operator	User	Configure User Accounts	Configure iRMC S2/S3 Settings	Video Redirection Enabled	Remote Storage Enabled
View *System Information...*	X	X	X	X				
View Chassis / M ainboard, / OS Information						X		
Set ASSET Tag[1)]						X		
Set System Name [1)]						X		
Set System Operating System Information[1)]						X		
Set System Description[1)]						X		
Set System Location Information (SNMP)[1)]						X		
Set System Contact Information (SNMP)[1)]						X		
Power Management...	X	X	X					
View *Enclosure Information*	X	X	X	X				
System Eventlog - *View/Dump System Eventlog*	X	X	X	X				
System Eventlog - *Clear System Eventlog*	X	X	X					
Internal Eventlog - *View/Dump Internal Eventlog*	X	X	X	X				
Internal Eventlog - *Clear Internal Eventlog*	X	X	X	X				
Sensor overviews (*Temperature, Fans ...*)	X	X	X	X				
View *Service Processor...*	X	X	X	X				
Service Processor... - *List IP Parameters*						X		

Table 9: Permissions to use the Remote Manager menus

Remote Manager menu items	Permitted with IPMI privilege level				Required permission			
	OEM	Administrator	Operator	User	Configure User Accounts	Configure iRMC S2/S3 Settings	Video Redirection Enabled	Remote Storage Enabled
Service Processor... - *Configure IP Parameters*						X		
Service Processor... - *Toggle Identify LED*	X	X	X	X				
Service Proc. ... - *Reset iRMC S2/S3 (warm/cold reset)*	X	X						
Change Password					X			
Console Redirection (EMS/SAC)	X	X	X					
Start a command Line shell...	X	X	X	X				
Console Logging	X	X	X					

[1] Action is only possible if no agents are running.

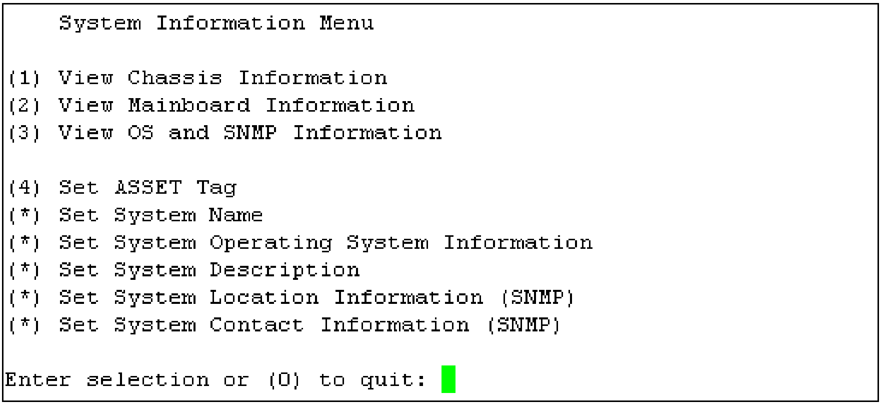
Table 9: Permissions to use the Remote Manager menus

8.7 Change the password

The *Change password* menu item allows a user with the privilege *Configure User Accounts* (see page 68) to change their own password or the passwords of other users.

8.8 System Information - Information on the managed server

The following menu appears if you choose *System Information...* from the main menu:



```
    System Information Menu

(1) View Chassis Information
(2) View Mainboard Information
(3) View OS and SNMP Information

(4) Set ASSET Tag
(*) Set System Name
(*) Set System Operating System Information
(*) Set System Description
(*) Set System Location Information (SNMP)
(*) Set System Contact Information (SNMP)

Enter selection or (0) to quit:
```

Figure 203: Remote Manager: System Information menu

The submenu contains the following functions:

View Chassis Information	Information on the chassis of the managed server and its product data.
View Mainboard Information	Information on the mainboard of the managed server and its product data.
View OS and SNMP Information	Information on the operating system and the ServerView version of the managed server and on the SNMP settings.

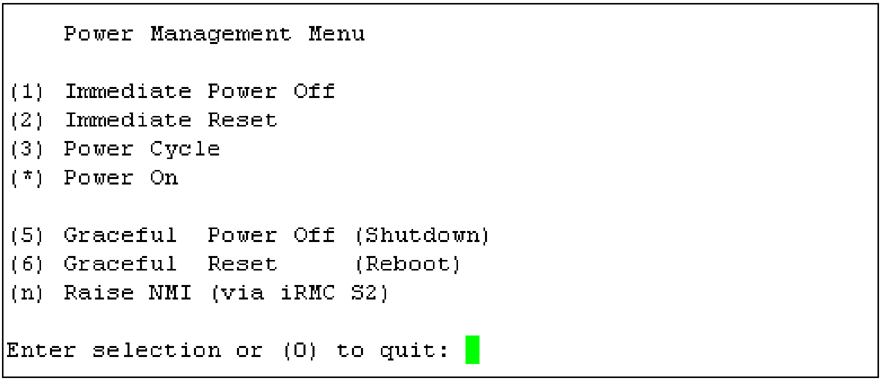
Table 10: System Information menu

Set ASSET Tag	Sets a customer-specific asset tag for the managed server.

Table 10: System Information menu

8.9 Power Management

The following menu appears if you choose *Power Management...* from the main menu:



```
    Power Management Menu

(1) Immediate Power Off
(2) Immediate Reset
(3) Power Cycle
(*) Power On

(5) Graceful  Power Off (Shutdown)
(6) Graceful  Reset     (Reboot)
(n) Raise NMI (via iRMC S2)

Enter selection or (0) to quit: 
```

Figure 204: Remote Manager: Power Management menu

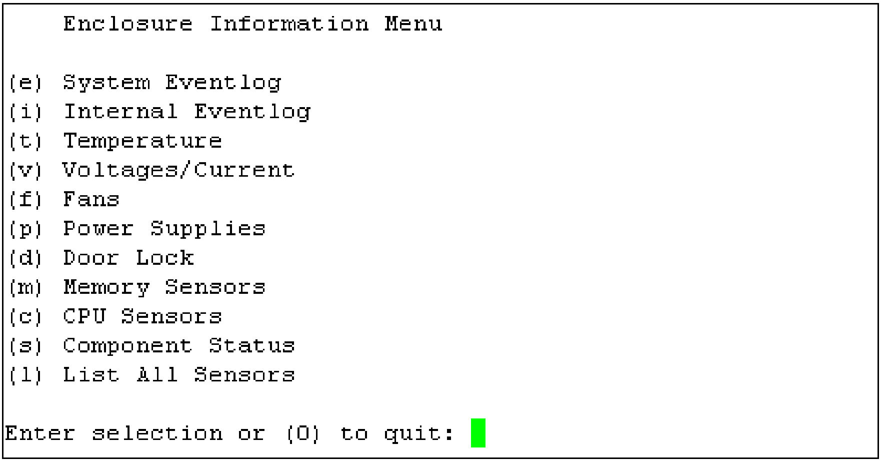
The submenu contains the following functions:

Immediate Power Off	Powers the server down, regardless of the status of the operating system.
Immediate Reset	Completely restarts the server (cold start), regardless of the status of the operating system.
Power Cycle	Powers the server down completely and then powers it up again after a configured period.
Power On	Switches the server on.
Graceful Power Off (Shutdown)	Graceful shutdown and power off. This menu item is only available if ServerView agents are installed and signed onto the iRMC S2/S3 as “Connected”.
Graceful Reset (Reboot)	Graceful shutdown and reboot. This menu item is only available if ServerView agents are installed and signed onto the iRMC S2/S3 as “Connected”.
Raise NMI (via iRMC S2/S3)	Initiates a non-maskable interrupt (NMI) via iRMC S2/S3

Table 11: Power Management menu

8.10 Enclosure Information - System event log and status of the sensors

The following menu appears if you choose *Enclosure Information...* from the main menu:



```
    Enclosure Information Menu

(e) System Eventlog
(i) Internal Eventlog
(t) Temperature
(v) Voltages/Current
(f) Fans
(p) Power Supplies
(d) Door Lock
(m) Memory Sensors
(c) CPU Sensors
(s) Component Status
(l) List All Sensors

Enter selection or (0) to quit: 
```

Figure 205: Remote Manager: Enclosure Information menu

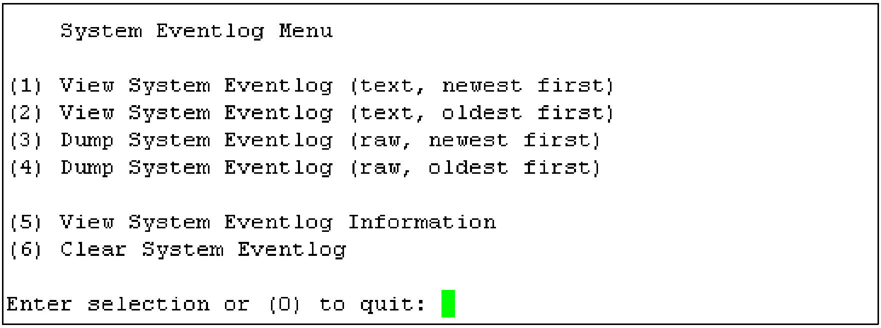
The submenu contains the following functions:

System Eventlog	Call the *System Eventlog* menu (see the section "System Eventlog" on page 337).
Internal Eventlog	Call the *internal Eventlog* menu (see the section "Internal Eventlog" on page 338).
Temperature	Display information on the temperature sensors and their status.
Voltages/Current	Display information on the voltage and current sensors and their status.
Fans	Display information on the fans and their status.
Power Supplies	Display information on the power supplies and their redundancy status.
Door Lock	Display information on whether the front panel or housing are open.
Memory Sensors	Display information on the memory statuses.
CPU Sensors	Localize the processors of the server.
Component Status	Display detailed information on all sensors that have a PRIMERGY diagnostic LED.
List All Sensors	Display detailed information on all sensors.

Table 12: Enclosure Information menu

System Eventlog

The following menu appears if you select *System Eventlog* from the *Enclosure Information...* submenu:



```
    System Eventlog Menu

(1) View System Eventlog (text, newest first)
(2) View System Eventlog (text, oldest first)
(3) Dump System Eventlog (raw, newest first)
(4) Dump System Eventlog (raw, oldest first)

(5) View System Eventlog Information
(6) Clear System Eventlog

Enter selection or (0) to quit:
```

Figure 206: Remote Manager: System Eventlog menu

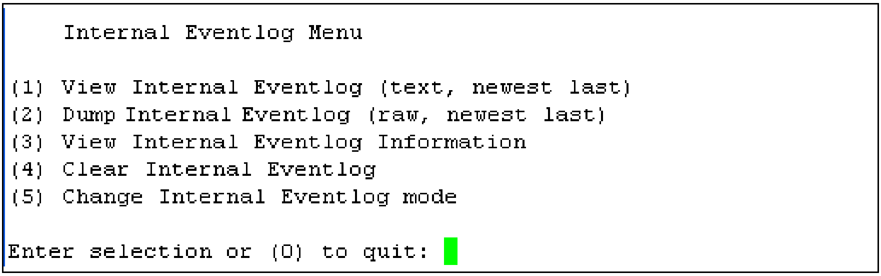
The submenu contains the following functions:

View System Eventlog (text, newest first)	The contents of the System Event log are output to screen in a readable form and in chronological order (the most recent entry first).
View System Eventlog (text, oldest first)	The contents of the System Event log are output to screen in a readable form and in reverse chronological order (the oldest entry first).
Dump System Eventlog (raw, newest first)	The contents of the System Event log are dumped in chronological order (the most recent entry first).
Dump System Eventlog (raw, oldest first)	The contents of the System Event log are dumped in reverse chronological order (the oldest entry first).
View System Eventlog Information	Display information on the System Event log.
Clear System Eventlog	Clear the contents of the System Event log.
Change System Eventlog mode	Changes the buffer mode of the System Event Log from *Ring Buffer* mode to *Linear Buffer* mode and vice versa.

Table 13: System Eventlog menu

Internal Eventlog

The following menu appears if you select *Internal Eventlog* from the *Enclosure Information...* submenu:



```
    Internal Eventlog Menu

(1) View Internal Eventlog (text, newest last)
(2) Dump Internal Eventlog (raw, newest last)
(3) View Internal Eventlog Information
(4) Clear Internal Eventlog
(5) Change Internal Eventlog mode

Enter selection or (0) to quit:
```

Figure 207: Remote Manager: Internal Eventlog menu

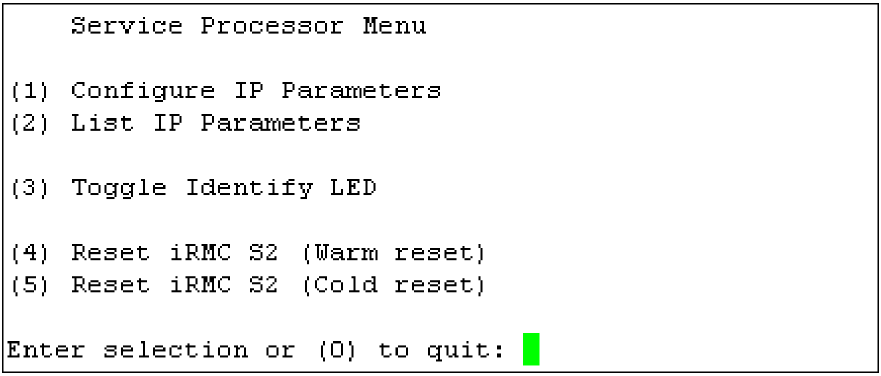
The submenu contains the following functions:

View Internal Eventlog (text, newest last)	The contents of the internal event log are output to screen in a readable form and in reverse chronological order (the most recent entry last).
Dump Internal Eventlog (raw, newest last)	The contents of the internal event log are dumped in reverse chronological order (the most recent entry last).
View Internal Eventlog Information	Display information on the internal event log.
Clear Internal Eventlog	Clear the contents of the internal event log.
Change Internal Eventlog mode	Changes the buffer mode of the internal event log from *Ring Buffer* mode to *Linear Buffer* mode and vice versa.

Table 14: Internal Eventlog menu

8.11 Service processor - IP parameters, identification LED and iRMC S2/S3 reset

The following menu appears if you choose *Service Processor...* from the main menu:



```
    Service Processor Menu

(1) Configure IP Parameters
(2) List IP Parameters

(3) Toggle Identify LED

(4) Reset iRMC S2 (Warm reset)
(5) Reset iRMC S2 (Cold reset)

Enter selection or (0) to quit: █
```

Figure 208: Remote Manager: Service Processor menu

The submenu contains the following functions:

Configure IP Parameters	Configure the IPv4 / IPv6 address settings of the iRMC S2/S3 in a guided dialog. Please refer to section "Network Interface Settings - Configure Ethernet settings on the iRMC S2/S3" on page 239 for details in the individual settings.
List IP Parameters	Display the IP settings.
Toggle Identify LED	Switch the PRIMERGY identification LED on/off.
Reset iRMC S2/S3 (Warm reset)	Reset the iRMC S2/S3. The connection is closed. Only the interfaces are re-initialized.
Reset iRMC S2/S3 (Cold reset)	Reset the iRMC S2/S3. The connection is closed. The entire iRMC S2/S3 is re-initialized.

Table 15: Service Processor menu

It is recommended that you reboot the server after a *Reset iRMC S2/S3 (Cold Reset)* or *Reset iRMC S2/S3 (Warm Reset)* (see page 189).

8.12 Console Redirection (EMS/SAC) - Start text console redirection

You can start console redirection with the *Console Redirection (EMS/SAC)* item from the main menu.

Text-based console redirection only works over the LAN with Serial 1.

If console redirection is also to be used while the operating system is running, the *Serial 1 Multiplexer* must be set to *System*.

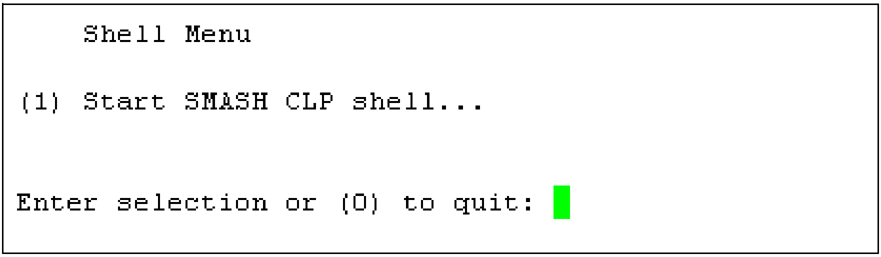
Use the keyboard shortcut "<ESC>(" or "~." (tilde dot) to exit the text console.

It is possible that only one of these options will work, depending on the type of PRIMERGY server used.

8.13 Start a Command Line shell... - Start a SMASH CLP shell

Start a Command Line shell... in the main menu allows you to start a SMASH CLP shell. SMASH CLP stands for "**S**ystems **M**anagement **A**rchitecture for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol". This protocol permits a Telnet- or SSH-based connection between the management station and the managed server. For further details on SMASH CLP, please refer to section "Command Line Protocol (CLP)" on page 343.

When you select *(s) Start a Command Line shell...* from the main menu, the following window appears:



```
    Shell Menu

(1) Start SMASH CLP shell...


Enter selection or (0) to quit:
```

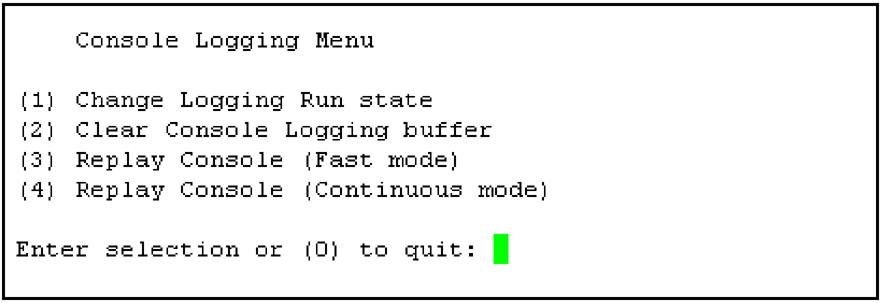
Figure 209: Remote Manager: Start a SMASH CLP shell... menu

► Choose *(1) Start a SMASH CLP shell...* to start the SMASH CLP shell.

8.14 Console Logging - Redirect message output to the text console (serial)

The *Console Logging* item in the main menu allows you to redirect message output (logging) to the text console (serial interface).

When you select *(l) Console Logging* from the main menu, the following window appears:



```
    Console Logging Menu

(1) Change Logging Run state
(2) Clear Console Logging buffer
(3) Replay Console (Fast mode)
(4) Replay Console (Continuous mode)

Enter selection or (0) to quit:
```

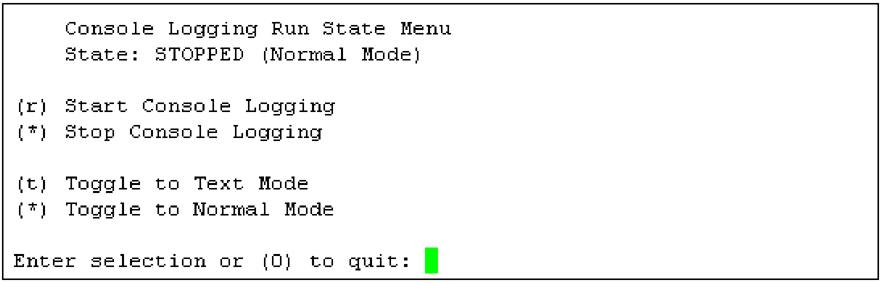
Figure 210: Remote Manager: Console Logging menu

The submenu contains the following functions:

Change Logging Run state	Show and change the logging run state. For a more detailed description, see "Console Logging Run State Menu" on page 342
Clear Console Logging buffer	Clear the console logging buffer.
Replay Console (Fast mode)	Show the console log (in fast mode)
Replay Console (Continuous mode)	Show the console log (in continuous mode)

Table 16: Console Logging menu

Console Logging Run State Menu



```
    Console Logging Run State Menu
    State: STOPPED (Normal Mode)

(r) Start Console Logging
(*) Stop Console Logging

(t) Toggle to Text Mode
(*) Toggle to Normal Mode

Enter selection or (0) to quit:
```

Figure 211: Remote Manager: Console Logging Run State menu

The *Console Logging Run State Menu* provides the following functions:

Start Console Logging	Start output of messages to the text console.
Stop Console Logging	Stop output of messages to the text console.
Toggle to Text Mode	Switch to text mode. All escape sequences are filtered out before messages are output to the console.
Toggle to Normal Mode	Switch to normal mode. In normal mode, only the following escape sequences are filtered out before messages are output to the console: <ESC>(<ESC>stop <ESC>Q <ESC>R<ESC>r<ESC>R <ESC>^ This means that color, pseudo-graphics, etc. can also be represented to a limited extent.

Table 17: Console Logging Run State menu

8.15 Command Line Protocol (CLP)

The iRMC S2/S3 supports various text-based user interfaces, known as user shells, which can be configured differently for individual users.

The **S**ystem **M**anagement **A**rchitecture for **S**erver **H**ardware (SMASH) initiative defines a number of specifications with the following objectives:

- Provision of standardized interfaces for managing heterogeneous computer environments,
- Provision of an architecture framework with uniform interfaces, hardware and software discovery, resource addressing and data models.

You can find further information on SMASH under the following link:

http://www.dmtf.org/standards/smash

SMASH CLP syntax

SMASH CLP specifies a common command line syntax and message protocol semantics for managing computers on the Internet and in enterprise and service provider environments. You can find detailed information on SMASH CLP in the DMTF document “Server Management Command Line Protocol Specification (SM CLP) DSP0214”.

The general syntax of the CLP is as follows:

```
<verb> [<options>] [<target>] [<properties>]
```

<verb>

Verbs specify the command or action to be executed. The list of verbs describes the following activities, for instance:

- Establish (*set*) and retrieve (*show*) data,
- Change the status of a target (*reset*, *start*, *stop*),
- Manage the current session (*cd*, *version*, *exit*),
- Return information on commands (*help*).

In iRMC S2/S3 systems, the verb *oemfujitsu* also allows the use of special OEM commands.

<options>

Command options modify the action or the behavior of a verb. Options can immediately follow the verb in a command line and must always be introduced by a dash ("-").

Options allow you to, for instance,

- define the output format,
- permit recursive execution of a command,
- display the version of a command or
- request help.

<target>

<target> specifies the address or the path of the object to be manipulated by the command, i.e. the target of the command. This can be a single managed element such as a hard disk, a network adapter (Network Interface Card, NIC), or the management program (Management Assistance Program, MAP) itself. Targets can, however, also be services such as a transport service.

Several managed elements which can be managed by the management program can be subsumed under a single <target>, for instance the entire system.

Only one <target> may be specified for each command.

<properties>

<properties> describe the properties of the target of the command which are required to execute the command. Thus, <properties> identify the properties of the target's class that are to be retrieved or modified by the command.

User data in the CLP (overview)

Data within the CLP is structured hierarchically. The command *cd* allows you to navigate within this structure.

An overview of the user data in the CLP is shown in figure 212. The names in rectangles indicate command targets. On every level of the hierarchy, the command/verb *show* displays the available targets, properties and verbs.

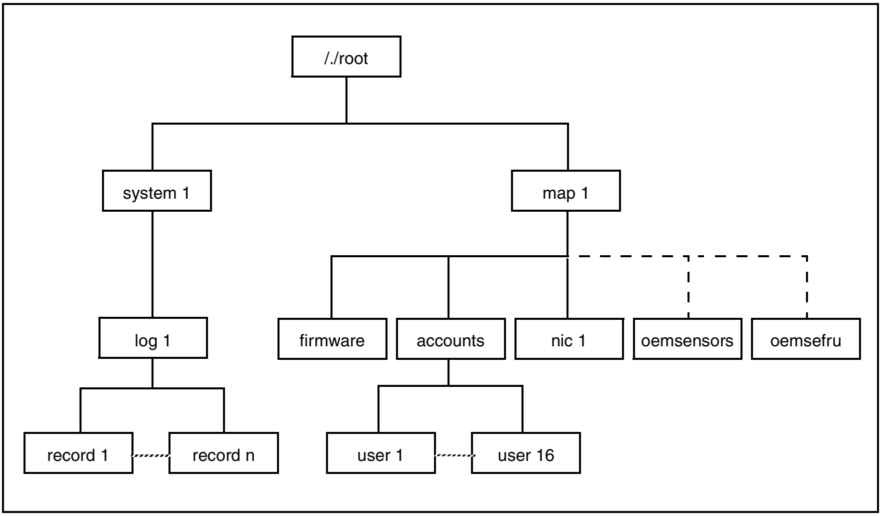
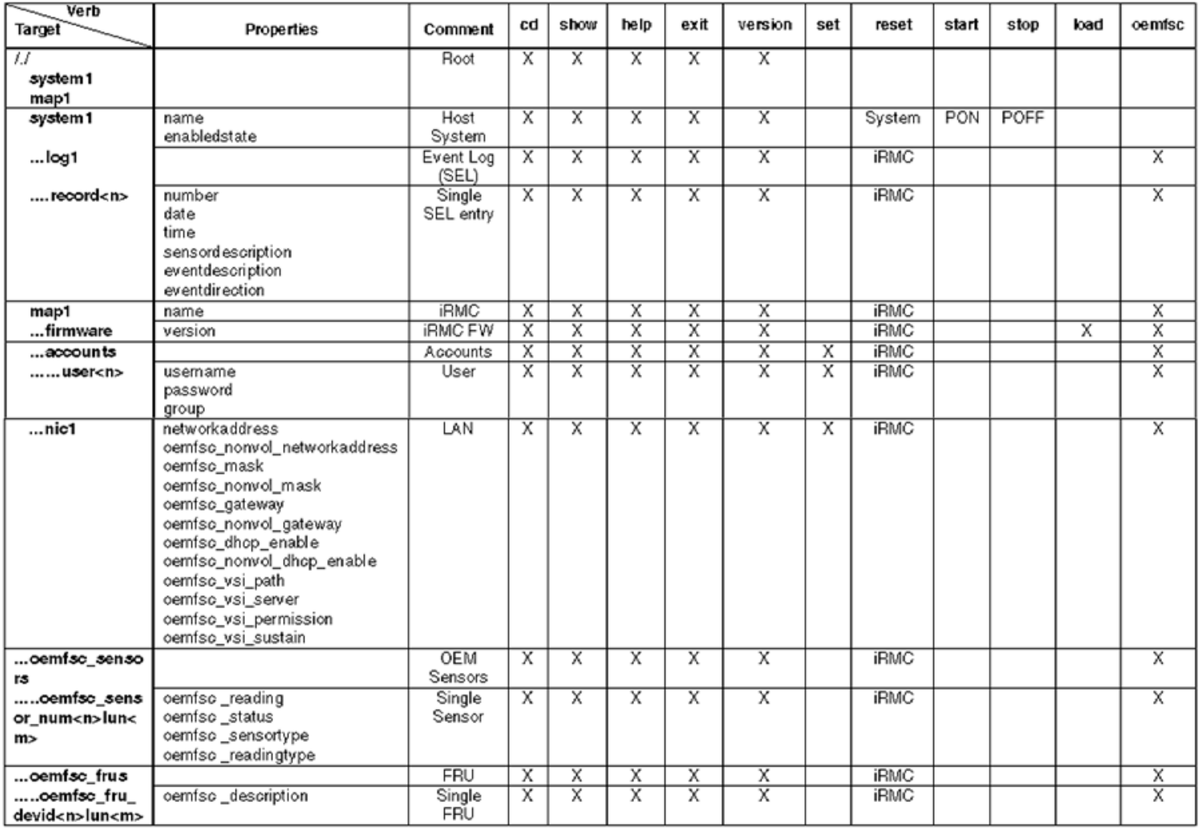


Figure 212: Structure of the user data in SMASH CLP

Hierarchy of the CLP commands

An overview of the CLP command hierarchy is shown in table 18 on page 346.



Verb / Target	Properties	Comment	cd	show	help	exit	version	set	reset	start	stop	load	oemfsc
/./ **system1** **map1**		Root	X	X	X	X	X						
system1	name enabledstate	Host System	X	X	X	X	X		System	PON	POFF		
...log1		Event Log (SEL)	X	X	X	X	X		iRMC				X
....record<n>	number date time sensordescription eventdescription eventdirection	Single SEL entry	X	X	X	X	X		iRMC				X
map1	name	iRMC	X	X	X	X	X		iRMC				X
...firmware	version	iRMC FW	X	X	X	X	X		iRMC			X	X
...accounts		Accounts	X	X	X	X	X	X	iRMC				X
......user<n>	username password group	User	X	X	X	X	X	X	iRMC				X
...nic1	networkaddress oemfsc_nonvol_networkaddress oemfsc_mask oemfsc_nonvol_mask oemfsc_gateway oemfsc_nonvol_gateway oemfsc_dhcp_enable oemfsc_nonvol_dhcp_enable oemfsc_vsi_path oemfsc_vsi_server oemfsc_vsi_permission oemfsc_vsi_sustain	LAN	X	X	X	X	X	X	iRMC				X
...oemfsc_sensors		OEM Sensors	X	X	X	X	X		iRMC				X
.....oemfsc_sensor_num<n>lun<m>	oemfsc _reading oemfsc _status oemfsc _sensortype oemfsc _readingtype	Single Sensor	X	X	X	X	X		iRMC				X
...oemfsc_frus		FRU	X	X	X	X	X		iRMC				X
.....oemfsc_fru_devid<n>lun<m>	oemfsc _description	Single FRU	X	X	X	X	X		iRMC				X

Table 18: Hierarchy of the CLP commands

9 Configuring iRMC S2/S3 using the Server Configuration Manager

You can use the Server Configuration Manager to

- configure the iRMC S2/S3,
- configure and manage user IDs at the iRMC S2/S3,
- configure a directory service on the iRMC S2/S3,
- configure the CAS service on the iRMC S2/S3.

Requirements:

The current ServerView agents must be installed on the managed server.

The Server Configuration Manager functions can be accessed in the following ways:

- Locally on managed servers using the ServerView Installation Manager.
- Locally on managed Windows-based servers using the Windows Start menu.

  This is only supported for servers on which the ServerView agents for Windows are installed.
- On the remote workstation using the graphical interface of the Operations Manager.

  This is only supported for servers on which the ServerView agents for Windows are installed.

This chapter in detail describes the various ways to call the Server Configuration Manager.

For details on the Configuration Manager dialog pages, please refer to the online help of the Server Configuration Manager.

9.1 Calling the Server Configuration Manager from the ServerView Installation Manager

You can call the Server Configuration Manager from the ServerView Installation Manager (Installation Manager for short). Configuration via the Installation Manager is of significance when installing the server. The Installation Manager makes the Server Configuration Manager available both during preparation for installation and as a separate maintenance program. The Installation Manager is described in the manual “ServerView Installation Manager”.

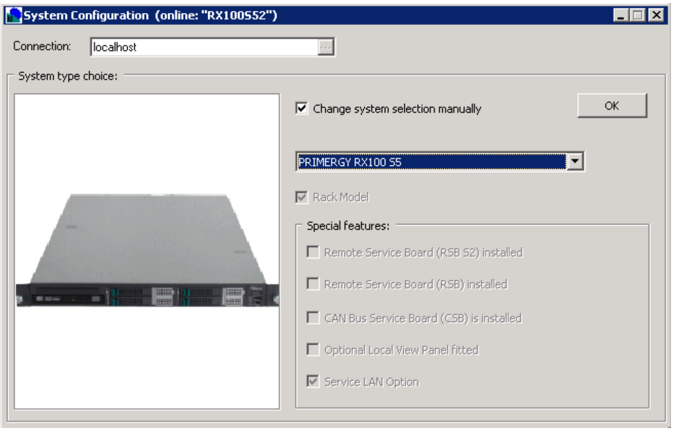
9.2 Calling the Server Configuration Manager from the Windows Start menu

On Windows-based servers, you can also call the Server Configuration Manager via the Windows Start menu.

To do this, proceed as follows:

► On the managed server, select:
Start – All Programs – Fujitsu – ServerView – Agents – Configuration Tools – System Configuration.

The *System Configuration* window opens:



System Configuration (online: "RX100S52")

Connection: localhost

System type choice:

☑ Change system selection manually

PRIMERGY RX100 S5

☑ Rack Model

Special features:

□ Remote Service Board (RSB S2) installed

□ Remote Service Board (RSB) installed

□ CAN Bus Service Board (CSB) is installed

□ Optional Local View Panel fitted

☑ Service LAN Option

Figure 213: System Configuration window

► Accept the preset values.

► Click *OK*.

The tab view of the *System Configuration* window opens.

You can scroll to the left and right through the tabs by clicking the arrows next to the tabs.

Applying settings

To apply the settings made in the individual tabs, proceed as follows for each tab:

► Click the *Apply* button.

► Click the *Save Page* button.

The iRMC S2/S3 automatically reboots to activate the changed settings.

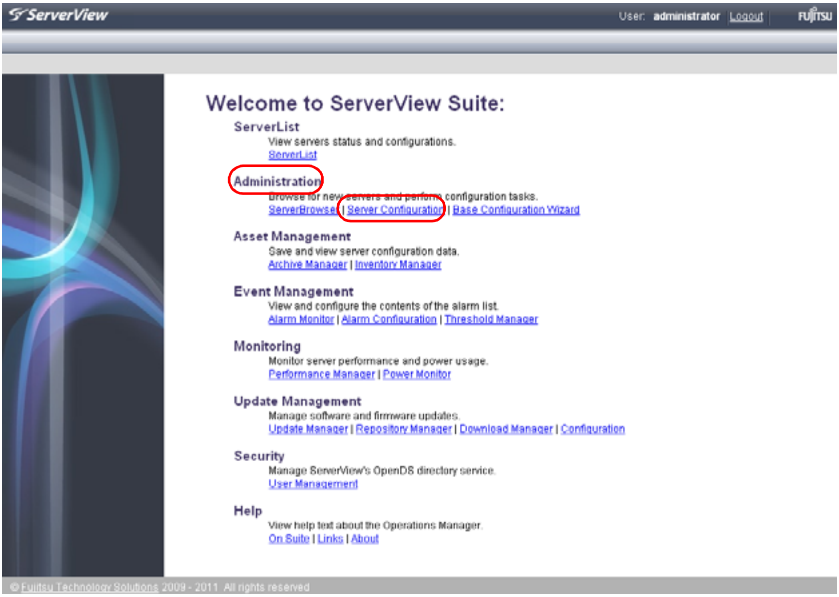
9.3 alling the Server Configuration Manager from the Operations Manager

The Server Configuration Manager dialog boxes for configuring the iRMC S2/S3 are also available from the graphical user interface of the Operations Manager. This allows you to configure the iRMC S2/S3 of the managed server from the remote workstation via a Web interface.

Proceed as follows:

► Start the Operations Manager (refer to the manual “ServerView Operations Manager”).

The start window of the Operations Manager opens:



Welcome to ServerView Suite:

ServerList
View servers status and configurations.
ServerList

Administration
Browse for new servers and perform configuration tasks.
ServerBrowser | Server Configuration | Base Configuration Wizard

Asset Management
Save and view server configuration data.
Archive Manager | Inventory Manager

Event Management
View and configure the contents of the alarm list.
Alarm Monitor | Alarm Configuration | Threshold Manager

Monitoring
Monitor server performance and power usage.
Performance Manager | Power Monitor

Update Management
Manage software and firmware updates.
Update Manager | Repository Manager | Download Manager | Configuration

Security
Manage ServerView's OpenDS directory service.
User Management

Help
View help text about the Operations Manager.
On Suite | Links | About

© Fujitsu Technology Solutions 2009 - 2011 All rights reserved

Figure 214: Operations Manager: Start window

► Choose *Server Configuration* from the *Administration* menu of the Operations Manager start window.

This opens the following window:

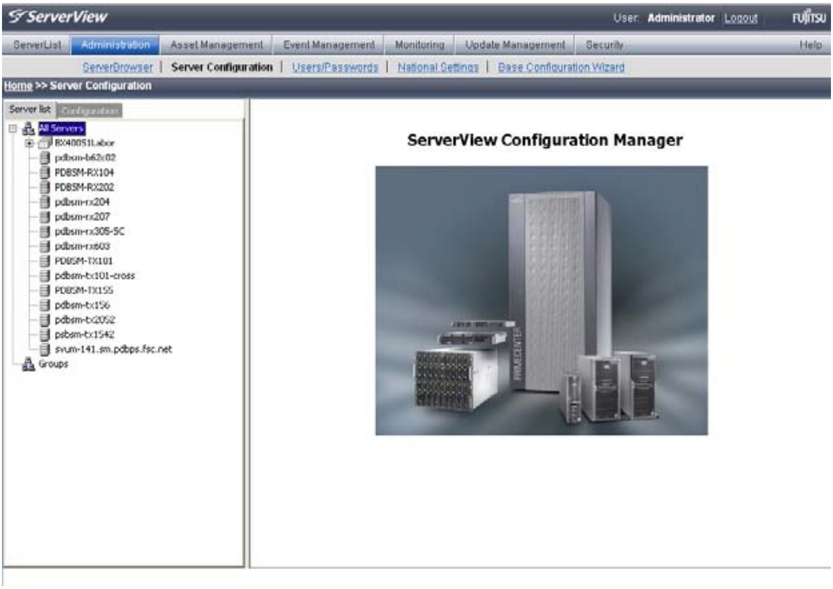
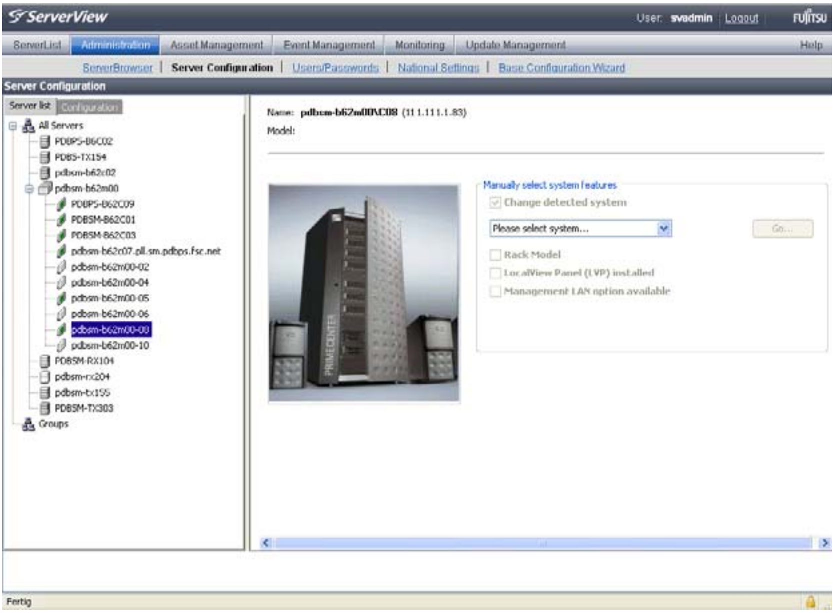


Figure 215: Operations Manager: Server Configuration window - Server list (1) tab

► In the hierarchy tree of the *Server list* tab, select the server to be configured.

This opens the following window:



Name: pdbsm-b62m00\C08 (11.111.1.83)

Model:

Manually select system features

☑ Change detected system

Please select system...

□ Rack Model

□ LocalView Panel (LVP) installed

□ Management LAN option available

Figure 216: Operations Manager: Server Configuration window - Server list (2) tab

► In the right-hand side of the window, specify the details on the selected server and confirm your entries by clicking *GO...* .

The first dialog of the Server Configuration manager appears.

10 Firmware update

This chapter provides you with information about the following topics:

- iRMC S2/S3 firmware (overview)
- Creating a memory stick for updating the firmware
- Updating firmware images
- Emergency flash
- flash tools

i The current firmware versions are present on the *ServerView Suite DVD 1* or can be downloaded manually from the Download section of the Fujitsu Technology Solutions web server.

You can obtain the up-to-date version of the *ServerView Suite DVD 1* at two-monthly intervals.

i Besides the possibility of performing a firmware update, you can also downgrade the firmware to the previous version.

i Before updating or downgrading the firmware, read the supplementary documentation supplied with the new firmware carefully (in particular the Readme files).

i Servers with iRMC S2 must be rebooted to activate the updated / downgraded firmware. For servers with iRMC S3, no reboot is required to activate the updated / downgraded firmware.

CAUTION!

When updating / downgrading the firmware, note that the problem-free operation of the firmware can only be guaranteed if the runtime firmware and the SDR (Sensor Data Record, see page 355) both belong to the same firmware release.

10.1 iRMC S2/S3 firmware (overview)

The iRMC S2/S3 uses two different firmware images. The two firmware images are stored on a 16-MB EEPROM (**E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory):

- Firmware image 1 (low FW image)
- Firmware image 2 (high FW image)

The firmware of the iRMC S2/S3 is not executed in the EEPROM, but is instead loaded into SRAM memory on startup and executed there. This means that it is possible to update both active and inactive firmware images online, i.e. with the server operating system (Windows or Linux) running.

ℹ If an error occurs while loading the firmware from one of the images, the firmware is automatically loaded from the other image.

ℹ Information on the iRMC S2/S3 firmware and EEPROM can be found

- in the iRMC S2/S3 web interface, page *iRMC S2/S3 Information* (see page 164) or
- using the flash tool (see page 368).

Active and passive firmware image

One of the two firmware images is active (running) at any given time, while the other is inactive. The firmware image that is active depends on the so-called firmware selector (see page 356).

Structure of the iRMC S2/S3 EEPROM

The EEPROM of the iRMC S2/S3 contains one area for firmware image 1 and one area for firmware image 2:

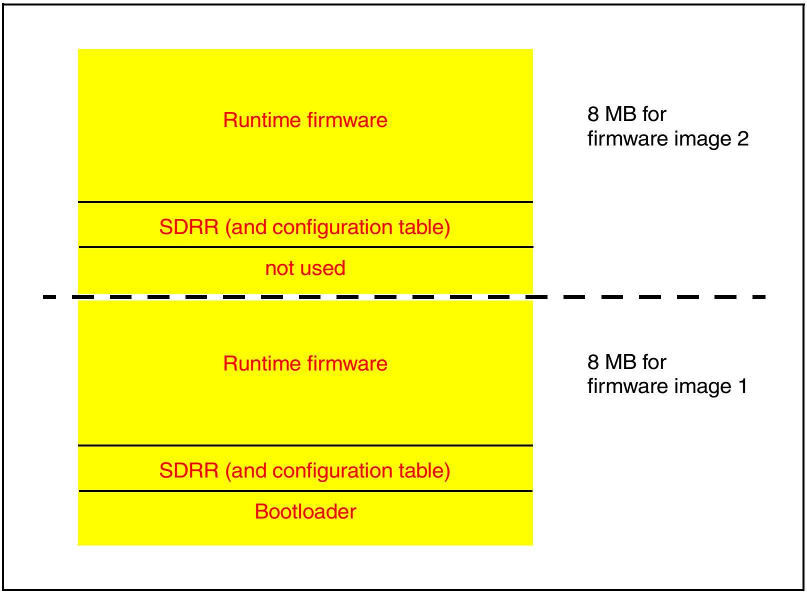

Runtime firmware
SDRR (and configuration table)
not used
8 MB for firmware image 2
Runtime firmware
SDRR (and configuration table)
Bootloader
8 MB for firmware image 1

Figure 217: Structure of the iRMC S2/S3 EEPROM

– Bootloader

  The bootloader checks the firmware image that is currently active. If a firmware error is detected, the bootloader sets the firmware selector to the other firmware image.

– SDRR (Sensor Data Record Repository)

  The SDRR contains the Sensor Data Records (SDR) in which sensor information for the managed server is stored. The SDRR also acts as an interface via which you can access the SDRs.

– Runtime firmware

  The runtime firmware is the executable part of the iRMC S2/S3's firmware.

You can perform a firmware update for each of these areas.

Firmware selector

The firmware selector specifies the iRMC S2/S3 firmware to be executed. Every time the iRMC S2/S3 is reset and restarted, the firmware selector is evaluated and processing branches to the corresponding firmware.

The firmware selector can have the following values:

0 Firmware image containing the most recent firmware version

1 firmware image 1

2 firmware image 2

3 Firmware image containing the oldest firmware version

4 Firmware image most recently updated

5 Firmware image that has been updated least recently

i Depending on the update variant used, the firmware selector is set differently after the update.

You can query and explicitly set the firmware selector

- on the *iRMC S2/S3 Information* page of the iRMC S2/S3 web interface (see "Running Firmware" on page 166)

  or

- using the flash tool (see page 368).

10.2 Setting up the USB memory stick

i You do **not** need the USB memory stick if you update the firmware of the iRMC S2/S3 in one of the following ways:

- using the ServerView Update Manager
- using ServerView Update Manager Express or ASP
- using the iRMC S2/S3 web interface and TFTP server

Proceed as follows:

► Download the firmware *iRMC Firmware Update for USB Stick* from the Download section of the Fujitsu Technology Solutions web server to a directory on your computer.

The ZIP archive *FTS_<spec>.zip* can be found in your download directory. (The *<spec>* part of the name provides information on the system type, system board, firmware/SDRR version etc.)

The ZIP archive includes the following files:

- *USBImage.exe*
- *iRMC_<Firmware-Version>.exe*
- *iRMC_<Firmware-Version>.IMA*

► Connect the USB memory stick to your computer.

► Start the file *iRMC_<Firmware-Version>.exe* or the file *USBImag.exe*.

One of the following windows is opened depending on the file you call (see figure 218 on page 358):

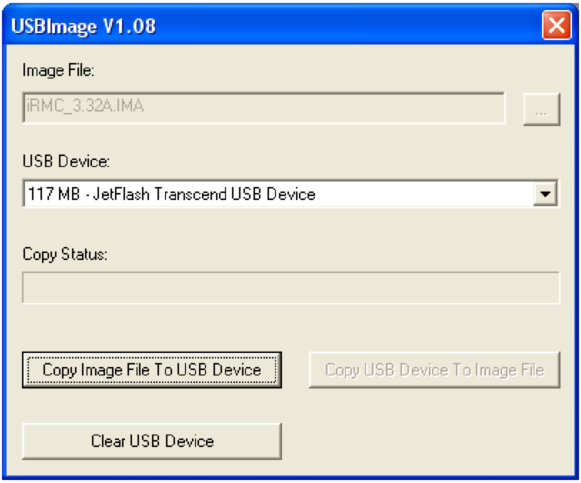


Image File: iRMC_3.32A.IMA

USB Device: 117 MB - JetFlash Transcend USB Device

Copy Status:

Figure 218: Copying the image file to the USB memory stick (with iRMC_<Firmware version.exe))

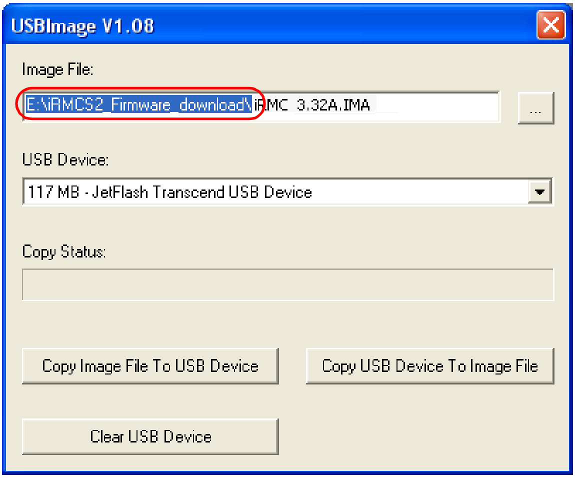


Image File: E:\iRMCS2_Firmware_download\iRMC_3.32A.IMA

USB Device: 117 MB - JetFlash Transcend USB Device

Copy Status:

Figure 219: Copying the image file to the USB memory stick (with USBImage.exe)

i If you have called *USBImag.exe*, then under *Image File:*, you must explicitly specify the file *iRMC_<Firmware-Version>.IMA*.

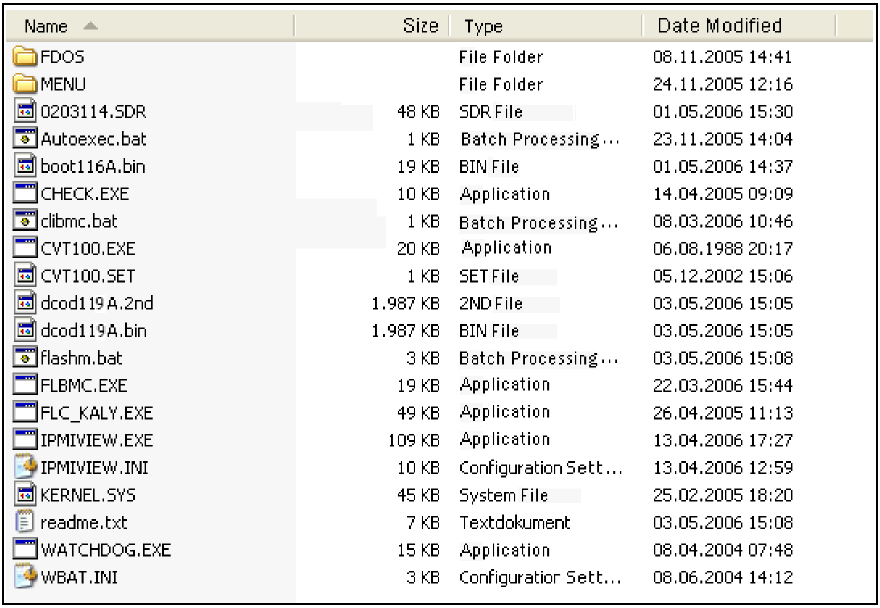
► Click *Clear USB Device* to delete the data from the USB memory stick.

► Click *Copy Image File to USB Device* to copy the file *BMC_<Firmware-Version>.IMA* to the USB memory stick and extract it.

CAUTION!

This action overwrites the content of the USB memory stick.

When the copy operation is complete, the flash tools and image files are present on the USB memory stick.



Name	Size	Type	Date Modified
FDOS		File Folder	08.11.2005 14:41
MENU		File Folder	24.11.2005 12:16
0203114.SDR	48 KB	SDR File	01.05.2006 15:30
Autoexec.bat	1 KB	Batch Processing...	23.11.2005 14:04
boot116A.bin	19 KB	BIN File	01.05.2006 14:37
CHECK.EXE	10 KB	Application	14.04.2005 09:09
clibmc.bat	1 KB	Batch Processing...	08.03.2006 10:46
CVT100.EXE	20 KB	Application	06.08.1988 20:17
CVT100.SET	1 KB	SET File	05.12.2002 15:06
dcod119A.2nd	1.987 KB	2ND File	03.05.2006 15:05
dcod119A.bin	1.987 KB	BIN File	03.05.2006 15:05
flashm.bat	3 KB	Batch Processing...	03.05.2006 15:08
FLBMC.EXE	19 KB	Application	22.03.2006 15:44
FLC_KALY.EXE	49 KB	Application	26.04.2005 11:13
IPMIVIEW.EXE	109 KB	Application	13.04.2006 17:27
IPMIVIEW.INI	10 KB	Configuration Sett...	13.04.2006 12:59
KERNEL.SYS	45 KB	System File	25.02.2005 18:20
readme.txt	7 KB	Textdokument	03.05.2006 15:08
WATCHDOG.EXE	15 KB	Application	08.04.2004 07:48
WBAT.INI	3 KB	Configuratior Sett...	08.06.2004 14:12

Figure 220: Image files and flash tool on the USB memory stick.

10.3 Updating firmware images

Since the iRMC S2/S3 firmware executes in the SRAM memory of the iRMC S2/S3, it is possible to update both active and inactive firmware images online, i.e. with the server operating system running.

The following methods are available for updating the firmware images:

- over the iRMC S2/S3 web interface
- using the ServerView Update Manager
- using ServerView Update Manager Express or ASP
- Update using the operating system flash tools.

Downgrading the firmware to the previous version

Besides the possibility of performing a firmware update, you can also downgrade the firmware to the previous version.

The simplest way to downgrade the firmware is to store the previous-version firmware image as the inactive firmware image in the EEPROM of the iRMC S2/S3. In this case, you only have to set the firmware selector to this previous-version image (see page 182) and subsequently restart the iRMC S2/S3 to activate the firmware.

You can also downgrade the firmware by applying the methods described in the following sections. In these cases, you perform a firmware update based on the firmware of the previous version. Special requirements to perform the downgrade are pointed out separately in the following sections.

10.3.1 Update via the iRMC S2/S3 web interface

The *iRMC S2/S3 Firmware Update* page allows you to update the firmware of the iRMC S2/S3 by providing the firmware image either locally on the remote workstation or on a TFTP server (see section "iRMC S2/S3 Firmware Update" on page 181).

10.3.2 Update using the ServerView Update Manager

Using the ServerView Update Manager, you can start the update of the iRMC S2/S3 firmware via a graphical user interface or via a command line interface (Windows and Linux). The ServerView Update Manager accesses the update data via its Update Repository on the *ServerView Suite DVD 1* or on the management server. You update the update repository on the management server by means of the Download Manager or by performing a manual download from the Download section of the Fujitsu Technology Solutions web server.

For more detailed information on firmware updates with the ServerView Update Manager, see the “ServerView Update Manager” manual.

10.3.3 Online update using ServerView Update Manager Express or ASP

Under Windows and Linux operating systems, you can update the iRMC S2/S3 firmware either using the graphical user interface of ServerView Update Manager Express or by using the ASP (Autonomous Support Package) command interface.

Under Windows, you can also start an ASP in the Windows Explorer by double-clicking the corresponding ASP-*\.*exe* file.

i **When downgrading the firmware, please note:**

- Downgrade via Update Manager Express:

  The firmware downgrade is only feasible in the *Expert* mode. In addition, the *Downgrade* option must be activated.

- Downgrade via ASP:

  - Under Windows:

    You can perform the downgrade if you start the ASP by double-clicking the corresponding **.exe* file. When starting the ASP via the CLI, you must explicitly specify the *Force=yes* option.

  - Under Linux:

    You must explicitly specify option *-f* or option *--force*.

For more detailed information on firmware updates with Update Manager Express and ASP, see the “Local System Update for PRIMERGY Servers” manual.

10.3.4 Update using the operating system flash tools.

An online update using the operating system flash tools is only performed as a recovery flash, i.e. no version check is performed.

Prerequisite:

The flash tools and the files for the firmware update must be present in the file system of the managed server.

You use one of the following flash tools, depending on the operating system you are running:

DOS:	flirmcs2
Windows:	winflirmcs2 **Prerequisite:** The ServerView agents for the used Windows operation system (32/64 bit) must be running on the managed server.
Windows (32 bit):	win32flirmcs2 (No agents required.)
Windows (64 bit):	win64flirmcs2 (No agents required.)
Linux:	linflirmcs2

You call the flash tools in the Windows command line (flirmcs2, win32flirmcs2, win64flirmcs2, winflirmcs2) or at the Linux CLI (linflirmcs2).

The syntax and operands for the flash tools are described in section "Flash tools" on page 368.

Proceed as follows:

i An online update using a USB memory stick is described below (see section "Setting up the USB memory stick" on page 357).

► Connect the USB memory stick to the managed server.

► In the Windows command line or the Linux Command Line Interface (CLI) switch to the drive corresponding to the USB memory stick.

► Set the firmware selector to the value 4 by calling the flash tool with the parameter */s 4*.

E.g., in the Windows command line you enter:

```
WinFLIRMCS2 /s 4
```

► Start the update of the firmware and the SDR data by calling the flash tool with the corresponding update files.

E.g., in the Windows command line you enter:

```
WinFLIRMCS2 dcod<firmware-version>.bin <nnnnnnn>.sdr /i
```

During the firmware update, the console informs you about the progress of the update operation. If an error occurs, the update operation is aborted and a corresponding return code is reported (see page 370).

► Restart the managed server. This automatically activates the firmware image with the updated firmware.

10.3.5 Update via the lashDisk menu

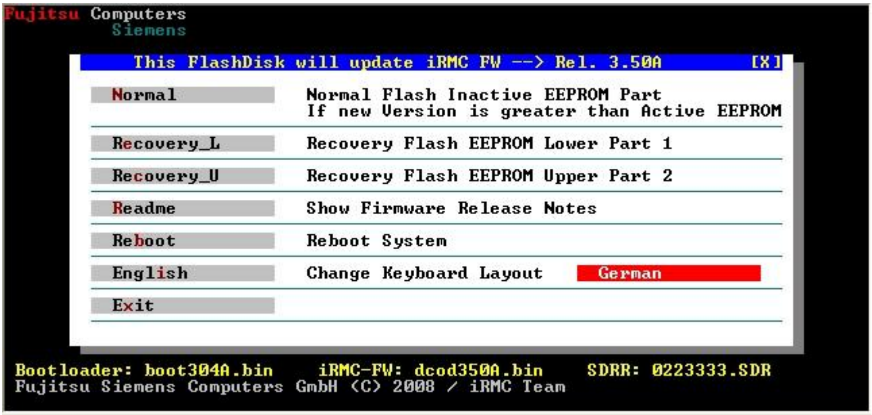
For an update via the FlashDisk menu, you require a bootable USB memory stick (see section "Setting up the USB memory stick" on page 357).

Proceed as follows:

- Connect the USB memory stick to the managed server (directly or via remote storage).
- Boot from the USB memory stick.

After completion of the boot operation, the data in the USB memory stick is automatically copied to a RAM disk. The *autoexec.bat* file is then started automatically.

The FlashDisk menu opens:



```
Fujitsu Computers
          Siemens

     This FlashDisk will update iRMC FW --> Rel. 3.50A          [X]

   Normal              Normal Flash Inactive EEPROM Part
                       If new Version is greater than Active EEPROM

   Recovery_L          Recovery Flash EEPROM Lower Part 1

   Recovery_U          Recovery Flash EEPROM Upper Part 2

   Readme              Show Firmware Release Notes

   Reboot              Reboot System

   English             Change Keyboard Layout     German

   Exit

Bootloader: boot304A.bin    iRMC-FW: dcod350A.bin    SDRR: 0223333.SDR
Fujitsu Siemens Computers GmbH (C) 2008 / iRMC Team
```

Figure 221: FlashDisk menu

A firmware downgrade is only possible via recovery flash.

Normal

A *normal flash* is performed.

During a normal flash operation, those areas of the EEPROM that contain the active firmware are checked to see whether they are up to date. If one of these areas is not up to date then the corresponding area for the inactive firmware is updated if it is not already up to date.

Recovery _L

A *recovery flash* for firmware image 1 (low firmware image) is carried out.

In the case of a recovery flash, the flash is performed for all three areas of firmware image 1 without any version check.

Recovery _U

A *recovery flash* for firmware image 2 (high firmware image) is carried out.

In the case of a recovery flash, the flash is performed for all three areas of firmware image 2 without any version check.

Readme

The Readme file is opened.

Reboot

An iRMC S2/S3 warm start is performed.

English / German

Specify keyboard layout. *German* is set by default.

- ► Start the required update variant by clicking on the corresponding button.

  During the firmware update, the console informs you about the progress of the update operation. If an error occurs, the update operation is aborted. A corresponding return code is reported (see page 370).

- ► Once the update operation has been completed, click on *Exit*, to close the FlashDisk menu.
- ► Remove the USB memory stick from the managed server.
- ► Restart the managed server (e.g. with Ctrl + Alt + Del).

10.4 Emergency flash

If the iRMC S2/S3 firmware can no longer be executed, e. g. because the SDRs are not compatible with the system, then you can use the emergency mode to start the firmware running again. In emergency mode, the system automatically branches to the bootloader and is the ready for the firmware update.

Emergency mode is indicated by the error LED (global error LED) (rot) and the identification LED (blue) flashing alternately.

To switch the managed server to emergency mode and then update the iRMC S2/S3's firmware, proceed as follows:

- Disconnect the power supply connector.
- Insert the connector in the socket again with the Identify key held down.

  The managed server is now in emergency mode.
- Boot the server to DOS and use the recovery flash procedure to update the iRMC S2/S3’s firmware.

  If the firmware is not active then the boot operation may take up to 2 minutes to start. You can ignore the error message “iRMC S2/S3 Controller Error” which the BIOS outputs during this period.

10.5 Flash tools

i The tools WinFLIRMCS2, rFLIRMCS2 and sFLIRMCS2 differ from flirmcs2 only in respect of the name and the environment in which they are called. This means that the description below also applies to WinFLIRMCS2, rFLIRMCS2 and sFLIRMCS2. Instead of “flirmcs2”, you simply enter “WinFLRMCS2”, “rFLIRMCS2” or “sFLIRMCS2” as appropriate.

Syntax

```
flirmcs2 {/v|/o [/4]|/s[<value>]}
```

```
flirmcs2 {<file1> [<file2>] [<file3>]
      [/n /l[<logfile>] /d /e /4 /i]}
```

```
flirmcs2 {/h|/?}
```

Options

/v Displays the current version of the command.

/o Displays the current versions of both firmware images.

/s Displays the value of the firmware selector.

/s <value>
Sets the value of the firmware selector. You use this option to define the firmware image from which the firmware is started after a firmware reset.

0 Sets the selector to the firmware image with the most recent firmware.

1 Sets the selector to firmware image 1.

2 Sets the selector to firmware image 2.

3 Sets the selector to the firmware image with the oldest firmware.

4 Sets the selector to the firmware image with the most recently updated firmware.

5 Sets the selector to the firmware image with the firmware which has not been updated for longest.

<file1> through <file3>

Specify one or more files to determine which updates are to be made: The following files are to be selected:

boot<FW-Version>.bin

Updates the bootloader firmware.

dcod<FW-Version>.bin

Updates the runtime firmware.

<SDR-Version>.SDR

Updates the SDR.

i To update firmware image 2, you must also specify option */4* (see below).

/4 Updating firmware image 2.

/l [<logfile>]

Outputs error messages to the specified log file. If no logfile is specified, the output is directed to the *flbmc.log* file.

/n No output on the console.
This option has priority over the */p* and */d* options.

/np A rotating bar is shown in place of the percentage completion during the flashing operation.

/d Outputs additional debug information.

/e Emulation mode (for debugging purposes only).

/i Update the inactive firmware.

/h and /?

Outputs help information.

Return values

0	Firmware update was executed successfully.
1	Illegal or missing arguments.
3	PROM type not available
4	Communication with iRMC S2/S3 not possible.
5	Incorrect binary file.
8	Error accessing Keyboard Control Style interface (KCS).
9	Timeout during communication with the target EEPROM.
10	No buffer allocated.
12	Network node busy.
13	Timeout erasing EEPROM.
14	Timeout flashing EEPROM.
15	Error erasing EEPROM.
16	Error flashing EEPROM.

11 Remote installation of the operating system via iRMC S2/S3

This chapter describes how you use the ServerView Installation Manager (abbreviated to Installation Manager below) and the iRMC S2/S3 features "Advanced Video Redirection (AVR)" and "Remote Storage" to install the operating system on the administered server from the remote workstation.

The chapter discusses the following specific topics:

- General procedure for the remote installation of an operating system using remote storage media.
- Booting the administered server from the remote workstation using ServerView DVD 1 (Windows and Linux).
- Installing Windows from the remote workstation after configuration on the administered server.
- Installing Linux from the remote workstation after configuration on the managed server.

The description focuses primarily on the handling of the remote storage media. It is assumed that readers are familiar with the Installation Manager functionality (see the manual "ServerView Installation Manager").

Prerequisites for the remote installation of the operating system via iRMC S2/S3:

- The iRMC S2/S3's LAN interface must be configured (see page 41).
- The license key for the use of the iRMC S2/S3 functions “Advanced Video Redirection (AVR)” and “Remote Storage” must be installed (see page 167).

11.1 Installing the operating system via iRMC S2/S3 - general procedure

For the Installation Manager, the remote installation of the operating system via iRMC S2/S3 represents a local configuration and installation of the operating system on the administered server which you perform from the remote workstation via the AVR window using remote storage media.

The following steps are required in order to perform an installation via the Installation Manager:

1. Connect the storage medium (DVD 1 or Installation Manager boot image) from which you want to boot as remote storage.
2. Boot and configure the managed server via DVD 1 or the Installation Manager boot image.
3. Use the Installation Manager at the remote workstation to install the operating system on the administered server.
4. Optimize mouse pointer synchronization in the AVR window (only necessary under Linux).

Installing Windows without the Installation Manager using the Windows installation CD/DVDs

You can perform a remote installation of Windows via Remote Storage either using the Installation Manager or exclusively using the Windows installation CD/DVDs. The two procedures correspond in terms of the handling of the remote storage media.

However, you are advised to install Windows via the Installation Manager for the following reasons:

– The Installation Manager itself identifies the required drivers and copies these to the system.

– All the Installation Manager functions are available to you during installation. This means that you can, for example, configure the entire system including the server management settings.

– Installations without the Installation Manager have to be controlled via the keyboard since the mouse cursor cannot be synchronized during the installation process. In contrast, if you install using the Installation Manager then all configuration and installation steps can be performed using the mouse.

- If you install without the Installation Manager then all the settings required for mouse cursor synchronization must subsequently be performed manually.
- Installation using the Installation Manager does not take significantly longer than installation using the operating system CD/DVDs.

Installing Linux without the Installation Manager using the Linux installation CD/DVD

If you know which drivers are required by the system then you can start the Linux installation by booting from the Linux installation CD/DVD.

If the installation requires you to integrate drivers from the floppy disk then, before starting the installation, you must set up a remote storage connection

- to the storage medium (CD-ROM/DVD-ROM or ISO image) from which you want to boot and
- if necessary to storage medium for driver installation.

11.2 Connecting a storage medium as remote storage

Remote Storage makes a “virtual” drive available which is located elsewhere in the network.

The source for the virtual drive can be:

- Physical drive or image file at the remote workstation. The image file may also be on a network drive (with drive letter, e.g. “D:” for drive D).
- Image file provided centrally in the network by means of a remote storage server.

Parallel remote storage connections:

The following are possible concurrently:

- **either up to two** Remote Storage connections to virtual drives at the remote workstation (if the connection is established over the AVR Java applet)

  or

- **one** Remote Storage connection to a Remote Storage server.

It is not possible to establish concurrent Remote Storage connections via an applet and via the Remote Storage server.

The *Remote Storage* page of the iRMC S2/S3 web interface allows you to obtain information on the status of the current remote storage connections (see page 312).

For detailed information on remote storage, see chapter "Remote Storage" on page 111.

Connecting a storage medium as remote storage at the remote storage workstation

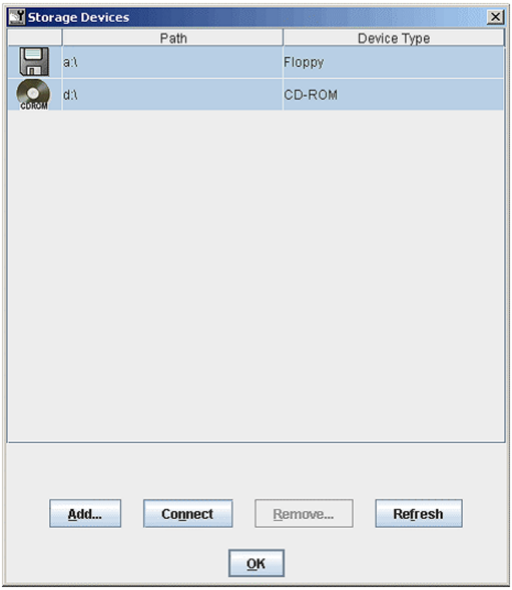
Proceed as follows at the remote workstation to establish the remote storage connection:

- ► Log into the iRMC S2/S3 web interface with Remote Storage Enabled permission (see page 136).
- ► Open the *Advanced Video Redirection (AVR)* page and start the AVR (see page 302).
- ► Start “Remote Storage” in the AVR window (see page 114).
- ► Prepare the storage media for remote storage (see page 117):
  - – If installation is performed via the Installation Manager:

    ServerView Suite DVD 1 or an Installation Manager boot image and optionally a formatted USB memory stick as a status backup medium.
  - – If installation is performed from the vendor’s installation CD/DVD: Windows or Linux installation CD/DVD and optional drivers.

  i It is recommended that the ServerView Suite DVD 1 and the operating system installation CD/DVD are stored in a folder as an image file (ISO image) and that they are connected from there as Remote Storage or provided via a Remote Storage server.

  The prepared storage media are displayed in the *Storage Devices* dialog box.



Storage Devices

	Path	Device Type
	a:\	Floppy
	d:\	CD-ROM

Figure 222: Storage Devices dialog box: ServerView Suite DVD 1

- Click *Connect* to connect the DVD ROM drive (DVD 1) or the Installation Manager boot image as remote storage.

Connect the ISO image (image file) provided by the remote storage server as remote storage

You can use an image file provided via the remote storage server for booting from an Installation Manager boot image.

i Before it is possible to use a virtual drive provided via a remote storage server, the remote storage server must be installed and started (see section "Providing remote storage via a Remote Storage server" on page 127).

To establish the connection to the remote storage server, proceed as follows at the remote workstation:

- Log into the iRMC S2/S3 web interface with *Remote Storage Enabled* permission (see page 136).
- Select the *Remote Storage* page.
- Establish the connection to the remote storage server (see page 314).

11.3 Booting the managed server from ServerView Suite DVD 1 and configuring it with the Installation Manager

Proceed as follows at the remote workstation:

► Use the iRMC S2/S3 web interface to start up the managed server or reboot the server (see page 189). You can follow the progress of the boot process in the AVR window.

During the managed server's BIOS/TrustedCore/UEFI POST phase, remote storage media are displayed as USB 2.0 devices. Remote Storage storage media are represented by the following entries in the BIOS boot sequence:

– A (physical) floppy disk is represented by a separate entry "FTS RemoteStorage FD-(USB 2.0)".

– All other remote storage device types are represented by the shared entry "CD-ROM DRIVE".

> If a local CD-ROM/DVD-ROM drive and a CD-ROM/DVD-ROM drive connected as remote storage are both present at the managed server then the managed server boots from the Remote Storage CD-ROM/DVD-ROM drive.

► Press [F2] while the server is booting.

► In the BIOS/TrustedCore/UEFI set-up, open the menu *Boot* in which you can define the boot sequence.

► Specify Boot Priority=1 (highest priority) for the ServerView Suite DVD 1 which is connected as remote storage.

► Save your settings and exit the BIOS/TrustedCore/UEFI setup.

The managed server then boots from ServerView Suite DVD 1 which is connected as remote storage.

> **If the system does not boot from the remote storage medium (ServerView Suite DVD 1 or Installation Manager boot image):**
>
> ► Check whether the storage medium is displayed during the BIOS POST phase and connect the storage medium as remote storage if necessary.
>
> ► Make sure that the correct boot sequence is specified.

It takes about 5 minutes to boot from ServerView Suite DVD 1 via a remote storage medium. The boot progress is indicated during the boot process. Once the boot process has completed, the Installation Manager startup displays a dialog box in which you are asked to select a medium for the status backup area (status backup medium).

> i Before you start to install the operating system, you should synchronize the local mouse cursor and the cursor of the managed server in the AVR window at the remote workstation. For more detailed information on synchronizing the mouse cursor in the AVR window, see section "Synchronizing the mouse pointer" on page 93.

- Choose *Standard mode* as the *Installation Manager mode*.
- Specify whether the configuration data is to be stored on a local replaceable data medium or on a network medium:

  > i Please note that if you do not select any status backup option all the configuration data is lost when you reboot.

  Status backup medium

  > i The backup medium must not be write-protected.
  >
  > A USB stick must already be connected to the USB port when the system is booted. If you fail to do this and wish to save the configuration file: Connect the USB stick now and reboot from ServerView Suite DVD 1.

  - Choose the option *on local drive (floppy / USB stick)*.
  - Select the corresponding drive in the box to the right of this option.

    For more detailed information on creating Installation Manager status disks, see the manual “ServerView Installation Manager”.

  Connecting the status medium and/or the installation media via the network

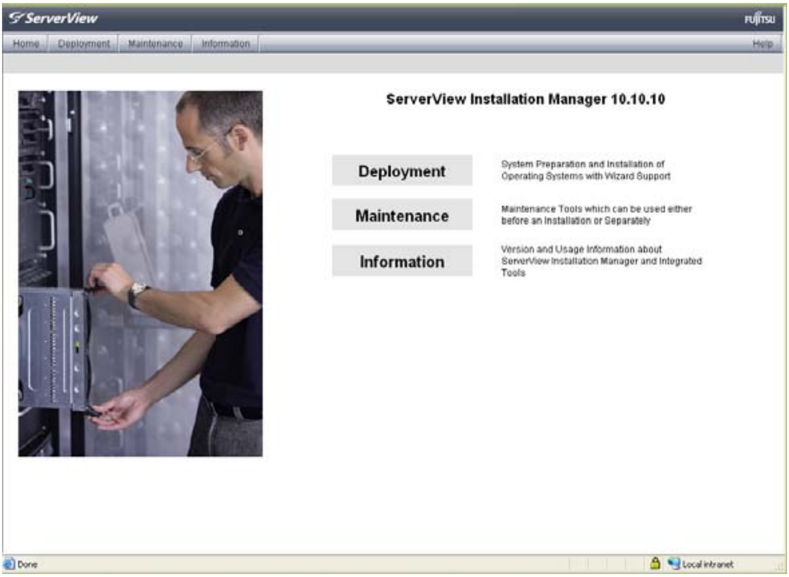
  - Set up the required shares for this purpose.

    > i If you are making a medium with a prepared configuration file and/or an installation medium available via the network, you have to choose this option. Depending on your infrastructure, you can either obtain a temporary IP address via DHCP or manually configure an IPv4 or IPv6 address for the current Installation Manager session.

- Start the Installation Manager by clicking *Continue*.

Starting local deployment

The Welcome screen appears when you start the Installation Manager:



ServerView Installation Manager 10.10.10

System Preparation and Installation of Operating Systems with Wizard Support

Maintenance Tools which can be used either before an Installation or Separately

Version and Usage Information about ServerView Installation Manager and Integrated Tools

Figure 223: Installation Manager - Welcome screen

► Click *Deployment* to start preparation of the local installation (deployment).

To prepare the installation, the Installation Manager wizards take you through a sequence of configuration steps that gather specifications for configuring the system and for subsequent unattended installation of the operating system.

i Configure the local CD ROM/DVD ROM drive of the managed server as the installation source. You can then also make the Windows installation CD/DVD available from the CD ROM/DVD ROM drive of the remote workstation if you connect it to the managed server as remote storage (see section "Installing Windows on the managed server after configuration" on page 380).

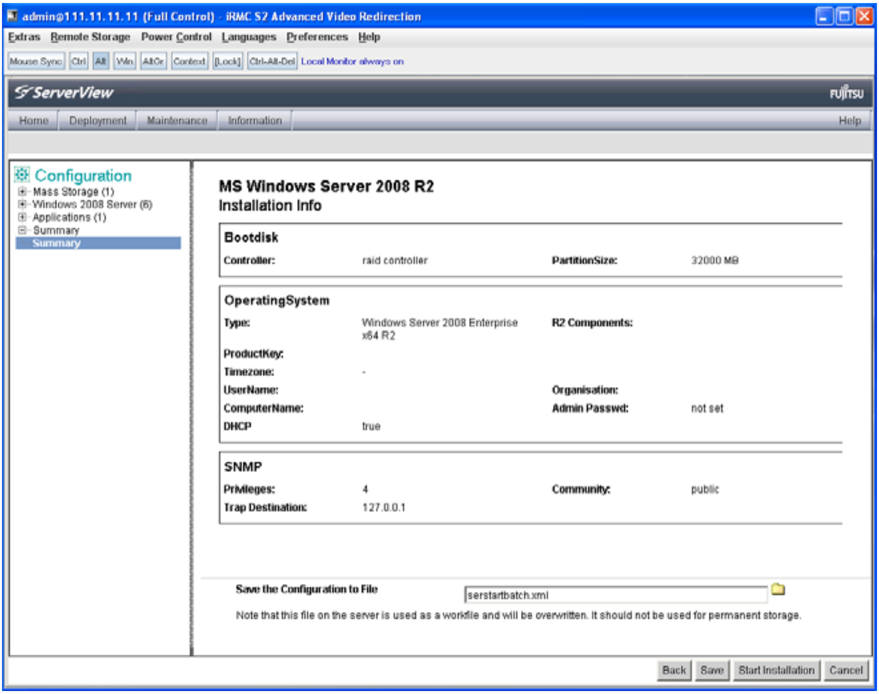
Once you have completed configuration with the Installation Manager, the *Installation Info* dialog page for the Windows installation (see page 380) or for the Linux installation (see page 383) is displayed. This allows you to start the installation process.

11.4 Installing the operating system on the managed server after configuration

Once you have completed configuration, you should install the operating system on the managed server.

11.4.1 Installing Windows on the managed server after configuration

After configuration has been completed, the Installation Manager displays the following dialog page:


admin@111.11.11.11 (Full Control) - iRMC S2 Advanced Video Redirection
Extras Remote Storage Power Control Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del Local Monitor always on
ServerView
FUJITSU
Home Deployment Maintenance Information Help
Configuration
Mass Storage (1)
Windows 2008 Server (6)
Applications (1)
Summary
Summary
Back Save Start Installation Cancel

MS Windows Server 2008 R2
Installation Info

Bootdisk

Controller:	raid controller	PartitionSize:	32000 MB

OperatingSystem

Type:	Windows Server 2008 Enterprise x64 R2	R2 Components:	
ProductKey:			
Timezone:	-		
UserName:		Organisation:	
ComputerName:		Admin Passwd:	not set
DHCP	true		

SNMP

Privileges:	4	Community:	public
Trap Destination:	127.0.0.1		

Save the Configuration to File: serstartbatch.xml

Note that this file on the server is used as a workfile and will be overwritten. It should not be used for permanent storage.

Figure 224: Installation Manager - Installation Info page

If you have configured the local CD ROM/DVD ROM drive of the managed server as the installation source, proceed as follows at the remote workstation:

- ► Clear your currently active remote storage connections. For more detailed information on clearing remote storage connections, see page 125.
- ► Remove ServerView Suite DVD 1 from the DVD ROM drive at the remote workstation.
- ► Insert the Windows installation CD/DVD in this DVD ROM drive.

  i Close the application if *autostart* is active.

- ► Connect the CD ROM/DVD ROM drive containing the Windows installation CD/DVD as remote storage (see page 121).
- ► In the *Installation Info* page of the Installation Manager, click *Start installation*.

  All the installation files are copied to the managed server.

  The Installation Manager opens a confirmation dialog page when the copy operation is complete and prompts you to remove all the storage media from the removable media drives before the managed server is rebooted.

  i Before rebooting the system, you must in particular shut down all current remote storage connections.

- ► To shut down all current remote storage connections, proceed as follows:
  - ► Start “Remote Storage” (see page 114).

    The *Storage Devices* dialog box is displayed with the currently connected storage devices and a “Safe Remove” indication.
  - ► “Safely remove” the storage device, i.e. ensure that no more applications/programs are accessing the storage media.
  - ► Click on *Disconnect...* to remove all the remote storage connections.
- ► On the confirmation dialog page, click *Ok* to reboot the managed server.

Once the managed server has rebooted, you can monitor the entire installation by means of the AVR.

For a Windows installation from the Windows installation CD/DVD:

To ensure perfect mouse cursor synchronization, you must adapt the following settings at the managed server once the operating system has been installed:

- Speed of the mouse pointer
- Hardware acceleration

For information on how to do this, see section "Managed Windows server: Adjusting the settings for synchronization of the mouse pointers" on page 95.

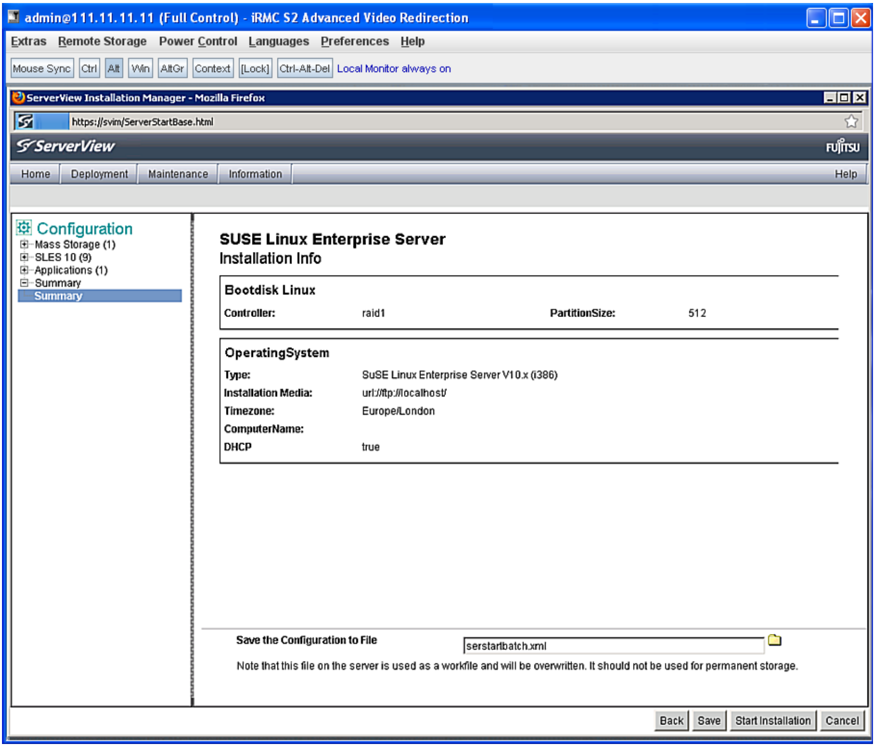
If Windows is installed using the Installation Manager, problem-free synchronization of the mouse pointers is automatically ensured.

11.4.2 Installing Linux on the managed server after configuration

The mouse can be used but not synchronized during Linux installation.

Whenever you change a remote storage medium, you must remove the remote storage connection for the currently connected medium and then connect the new medium as remote storage.

After configuration has been completed, the Installation Manager displays the following dialog page:


admin@111.11.11.11 (Full Control) - iRMC S2 Advanced Video Redirection
Extras Remote Storage Power Control Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del Local Monitor always on
ServerView Installation Manager - Mozilla Firefox
https://svim/ServerStartBase.html
ServerView
FUJITSU
Home Deployment Maintenance Information Help
Configuration
Mass Storage (1)
SLES 10 (9)
Applications (1)
Summary
Summary
Back Save Start Installation Cancel

SUSE Linux Enterprise Server
Installation Info

Bootdisk Linux

Controller:	raid1	PartitionSize:	512

OperatingSystem

Type:	SuSE Linux Enterprise Server V10.x (i386)
Installation Media:	url://ftp://localhost/
Timezone:	Europe/London
ComputerName:	
DHCP	true

Save the Configuration to File: serstartbatch.xml

Note that this file on the server is used as a workfile and will be overwritten. It should not be used for permanent storage.

Figure 225: Installation Manager - Installation Info

If you have configured the local CD ROM/DVD ROM drive of the managed server as the installation source, proceed as follows at the remote workstation:

- Clear your currently active remote storage connections. For more detailed information on clearing remote storage connections, see page 125.
- Remove ServerView Suite DVD 1 from the DVD ROM drive at the remote workstation.
- Insert the Linux installation CD/DVD in this DVD ROM drive.

  i Close the application if *autostart* is active.

- Connect the CD ROM/DVD ROM drive containing the Linux installation CD/DVD as remote storage (see page 121).
- In the *Installation Info* page of the Installation Manager, click *Start installation*.

  All the installation files are copied to the managed server. The Installation Manager opens a confirmation dialog page when the copy operation is complete and prompts you to remove all the storage media from the removable media drives before the managed server is rebooted.

  i Before rebooting the system, you must in particular shut down all current remote storage connections.

- Before rebooting the system, shut down the current remote storage connections.

  To do this, proceed as follows:

  - Start “Remote Storage” (see page 114).

    The *Storage Devices* dialog box is displayed with the currently connected storage devices and a “Safe Remove” indication.

  - Click on *Disconnect...* to remove all the remote storage connections.
  - “Safely remove” the storage device, i.e. ensure that no more applications/programs are accessing the storage media.

- On the confirmation dialog page, click *Ok* to reboot the managed server.

Once the managed server has rebooted, you can monitor the entire installation by means of the AVR.

i To ensure perfect mouse cursor synchronization, you must adapt the required settings at the managed server once the operating system has been installed. For information on how to do this, see section "Managed Linux server: Adjusting the settings for synchronization of the mouse pointers" on page 98.

12 Appendix

The appendix provides you with information about the following topics:

– "IPMI OEM Commands supported by the iRMC S2/S3" on page 385

– "Configuring the iRMC S2/S3 via SCCI and scripted configuration" on page 412

12.1 IPMI OEM Commands supported by the iRMC S2/S3

This section describes a selection of OEM-specific IPMI commands supported by the iRMC S2/S3.

12.1.1 Overview

The following OEM-specific IPMI commands are supported by the iRMC S2/S3:

- SCCI-compliant Power On/Off commands
  (SCCI: **S**erverView **C**ommon **C**ommand **I**nterface)
  - 0115 Get Power On Source
  - 0116 Get Power Off Source
  - 011C Set Power Off Inhibit
  - 011D Get Power Off Inhibit
  - 0120 Set Next Power On Time
- **SCCI-compliant communication commands**
  - 0205 System OS Shutdown Request
  - 0206 System OS Shutdown Request and Reset
  - 0208 Agent Connect Status
  - 0209 Shutdown Request Canceled
- **SCCI-compliant signaling commands**
  - 1002 Write to System Display

- **Firmware-specific commands**
  - 2004 Set Firmware Selector
  - 2005 Get Firmware Selector
  - C019 Get Remote Storage Connection
  - C01A Set Video Display on/off
- **BIOS-specific command**
  - F109 Get BIOS POST State
  - F115 Get CPU Info
- **iRMC S2/S3-specific commands**
  - F510 Get System Status
  - F512 Get EEPROM Version Info
  - F542 Get HDD lightpath status (Component Status Signal Read)
  - F543 Get SEL entry long text
  - F545 Get SEL entry text
  - F5B0 Set Identify LED
  - F5B1 Get Identify LED
  - F5B3 Get Error LED
  - F5DF Set Nonvolatile Cfg Memory to Default Values
  - F5E0 Set Configuration Space to Default Values
  - F5F8 Delete User ID

12.1.2 Description of the IPMI OEM commands

The following sections describe the individual OEM-specific IPMI commands.

12.1.2.1 Description format

The OEM-specific IPMI commands contained in this chapter are described in the format used by the IPMI standard for describing IPMI commands.

The IPMI standard describes the IPMI commands using command tables which list the input and output parameters for each command.

You can find information on the IPMI standards on the Internet under:

http://developer.intel.com/design/servers/ipmi/index.htm

12.1.2.2 SCCI-compliant Power On/Off commands

01 15 - Get Power On Source

This command returns the reason for the most recent Power On. The possible reasons are listed below.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**15** Command Specifier
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	3	**01** Data Length
	4	Power on Source: Cause of last power on

Power on Source	Description
0x00	Software or command
0x01	Power switch (on the front panel or keyboard)
0x02	Automatic restart after power failure
0x03	Clock or timer (hardware RTC or software timer)
0x04	Automatic restart after fan failure shutdown
0x05	Automatic restart after critical temperature shutdown
0x08	Reboot after watchdog timeout
0x09	Remote on (modem RI line, SCSI termination power, LAN, chip card reader...)
0x0C	Reboot after a CPU error
0x15	Reboot by hardware reset
0x16	Reboot after warm start
0x1A	Powered on by a PCI Bus Power Management Event
0x1D	Powered on by remote control via remote manager
0x1E	Reboot/reset by remote control via remote manager

01 16 - Get Power Off Source

This command returns the reason for the most recent Power Off. The possible reasons are listed below.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**16** Command Specifier
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	3	**01** Data Length
	4	Power off Source: Cause of last power off

Power off Source	Description
0x00	Software (SWOFF, power off by command)
0x01	Power switch (on the front panel or keyboard)
0x02	AC power fail
0x03	Clock or timer (hardware RTC or software timer)
0x04	Fan failure
0x05	Critical temperature
0x08	Final power-off after repeated watchdog timeouts
0x0C	Final power-off after repeated CPU errors
0x1D	Powered off by remote control via remote manager

01 1C - Set Power Off Inhibit

This command sets the *Power Off Inhibit* flag, which temporarily suppresses any unfounded attempt to power down the server.

If the *Power Off Inhibit* flag is set, the firmware saves the cause of any attempt to perform a “Power Off”, “Power Cycle” or restart of the server, but does not perform the action. The cause of the most recent attempt to perform a “Power Off”, “Power Cycle” or restart of the server is always saved at any given time. The stored action is only performed when the *Power Off Inhibit* flag is reset.

The *Power Off Inhibit* flag is automatically reset after a power failure or when the reset button is pressed.

The effect of the *Power Off Inhibit* flag is the same as that of the Dump flag used when creating a main memory dump. In this case, the initiator must set the flag before making the dump and reset it when the dump is complete.

Request Data	-	**B8** NetFn|LUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**1C** Command Specifier
	5	**00** Object ID
	6:7	**00 00** Value ID
	8	**01** Data Length
	9	Power Off Inhibit Flag: 0 no Inhibit, 1 Inhibit
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

01 1D - Get Power Off Inhibit

This command gets the value of the *Power Off Inhibit* flag.

For further details on the *Power Off Inhibit* flag, see the description of "01 1C - Set Power Off Inhibit" on page 390

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**1D** Command Specifier
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	**01** Response Data Length
	6	Power Off Inhibit Flag: 0 no Inhibit, 1 Inhibit

01 20 - Set Next Power On Time

This command switches on a system at the given time independent of the stored On/Off times in the Configuration Space.

The command takes effect only once.

You cancel a “Power On” time previously set with a 01 20 command by specifying the “Power On” time “0” in a subsequent 01 20 command.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**20** Command Specifier
	5	**00** Object ID
	6:7	**00 00** Value ID
	8	**04** Data Length
	9:12	Time (LSB first) (see below)
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first

Time (LSB first)

Time (UNIX-specific format) when the system switches on again. Time is NOT stored in non-volatile memory. Resolution is 1 minute. After the system has switched on, Time is set to 0 internally.
If Time == 0, the system is not switched on.

12.1.2.3 SCCI-compliant communication commands

Die SCCI-compliant communication commands require that the Agent Service is running under the OS. To execute the commands, the iRMC S2/S3 communicates with Agent which finally performs the action.

02 05 - System OS Shutdown Request

This command initiates shutdown of the server’s operating system.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**05** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first

02 06 - System OS Shutdown Request and Reset

This command initiates the shutdown of the server’s operating system and subsequently restarts the system.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**06** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first

02 08 - Agent Connect Status

This command checks whether the agent is active.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**08** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	5	**01** Data Length
	6	**Connect Status:** 00 = Connection lost, agent not connected. 01 = Connection re-established, agent connected.

02 09 Shutdown Request Cancelled

This command cancels a shutdown request that has been issued.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**09** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first

12.1.2.4 SCCI-compliant signaling command

10 02 - Write to System Display

This command is used to write characters to the LocalView display (if connected).

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**10** Cmd : Command Group Fan Test
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**02** Command Specifier
	5	**Object Index**: : Line on Display to write on.
	6:7	**Value ID** (not used)
	8	**Length** Number of characters to write, incremented by one. (The string need not be null-terminated; characters exceeding the length of a display line are truncated.)
	9	**Attribute:** 0 = Write String left aligned. 1 = Write String centered.
	10:10+n	**Characters** to write to the display; string need not be null-terminated.
Response Data	-	**BC**
	-	**10**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first

12.1.2.5 Firmware-specific commands

20 04 - Set Firmware Selector

This command configures the firmware image of the iRMC S2/S3 which is to be active after a firmware reset.

Request Data	-	**20** NetFnlLUN: Firmware
	-	**04** CMD : Command Group Firmware
	1	Selector: 0 = Auto (Select firmware image with highest firmware version.) 1 = low firmware image 2 = high firmware image 3 = Auto oldest version (Select firmware image with oldest firmware version.) 4 = MRP (Select most recently programmed firmware.) 5 = LRP (Select least recently programmed firmware.)
Response Data	-	**24**
	-	**04**
	1	Completion Code

20 05 - Get Firmware Selector

This command returns the current firmware selector setting.

Request Data	-	**20** NetFnlLUN: Firmware
	-	**05** CMD : Command Group Firmware
Response Data	-	**24**
	-	**05**
	1	Completion Code
	2	Next Boot Selector: 0 = Auto (Select EEPROM with highest firmware version.) 1 = low EEPROM 2 = high EEPROM 3 = Auto oldest version (Select EEPROM oldest firmware version.) 4 = MRP (Select most recently programmed firmware.) 5 = LRP (Select least recently programmed firmware.)
	3	Running Selector; tells which firmware is currently running: 1 = low EEPROM 2 = high EEPROM

C0 19 - Get Remote Storage Connection or Status

Depending on the parameters passed, this command returns information on

- whether any Remote Storage connections are available,
- the status and type of any Remote Storage connection(s).

If *Request Data 1* is set to “1”, the command returns information as to whether storage media are connected as Remote Storage.

Request Data	-	**C0** NetFnlLUN: OEM
	-	**19** CMD : Command Group Firmware
	1	01
	2	00
	3	00
Response Data	-	**C4**
	-	**19**
	1	Completion Code
	2	**01**
	3	**00: No** **01: Yes, connected**
	4	**00**
	5	**00**

If *Request Data 1* is set to “2”, the command returns information on the status and type of any Remote Storage connection(s).

Request Data	-	**C0** NetFnlLUN: OEM
	-	**19** CMD : Command Group Firmware
	1	02
	2	00
	3	00 = Connection 0 01 = Connection 2
Response Data	-	**C4**
	-	**19**
	1	Completion Code
	2	**02**
	3	**00**
	4	**00**
	5	**00 = Invalid / unknown** **01 = idle** **02 = Connection Attempt pending** **03 = Connected** **04 = Connection Attempts retries exhausted / failed** **05** = **Connection lost** **06** = **Disconnect pending**
	6	00 **= Invalid / unknown** **01 = Storage Server / IPMI** **02 = Applet** **03 = None / Not connected**

C0 1A - Set Video Display On/Off

This command allows you to switch the local console on or off.

Request Data	-	**C0** NetFnlLUN: OEM
	-	**1A** Cmd : Command Group Fan Test
	1	00 = Set Video Display On 01 = Set Video display Off
Response Data	-	**C4**
	-	**1A**
	1	Completion Code

12.1.2.6 BIOS-specific commands

F1 09 - Get BIOS POST State

This command provides information whether BIOS is in POST.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F1** Cmd : Command Group BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**09** Command Specifier
Response Data	-	**BC**
	-	**F1**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	[7:1] - reserved [0] - BIOS POST State : 0 = BIOS is not in POST 1 = BIOS is in POST

F1 15 - Get CPU Info

This command returns CPU-internal information. The iRMC S2/S3 gets this information from the BIOS during the POST phase.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F1** Cmd : Command Group BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**15** Command Specifier
	5	Socket Number (0-based) of the CPU
Response Data	-	**BC**
	-	**F1**
	1	**Completion Code:** 01 = Unpopulated CPU Socket
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5:6	CPU ID, LS Byte first
	7	Platform ID
	8	Brand ID
	9:10	Maximal Core Speed of the CPU [MHz], LS Byte first
	11:12	Intel Qickpath Interconnect in Mega Transactions per second, LS Byte first
	13	T-Control Offset
	14	T-Diode Offset
	15	CPU data Spare
	16:17	Record ID CPU Info SDR, LS Byte first
	18:19	Record ID Fan Control SDR, LS Byte first
	20:21	CPU ID High Word, LS Byte first (0 if none)

12.1.2.7 iRMC S2/S3-specific commands

F5 10 - Get System Status

This command returns a variety of internal information on the system such as the power state, error status, etc.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group Memory
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**10** Command Specifier
	5:8	**Timestamp**
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	5	**System Status** (For details see below.)
	6	**Signaling** (For details see below.)
	7	**Notifications** (For details see below.)
	8	**POST Code**

The Timestamp is only relevant for evaluating the *Notifications* Byte.

System Status

Bit 7 - System ON

Bit 6 -

Bit 5 -

Bit 4 - SEL entries available

Bit 3 -

Bit 2 - Watchdog active

Bit 1 - Agent connected

Bit 0 - Post State

Signaling

Bit 7	-	Localize LED
Bit 6	-	
Bit 5	-	
Bit 4	-	
Bit 3	-	CSS LED
Bit 2	-	CSS LED
Bit 1	-	Global Error LED
Bit 0	-	Global Error LED

Notifications

Bit 7	-	SEL Modified (New SEL Entry)
Bit 6	-	SEL Modified (SEL Cleared)
Bit 5	-	SDR Modified
Bit 4	-	Nonvolatile IPMI Variable Modified
Bit 3	-	ConfigSpace Modified
Bit 2	-	
Bit 1	-	
Bit 0	-	New Output on LocalView display

F5 12 - Get EEPROM Version Info

This command returns information on the current versions (bootloader, firmware and SDR) stored in the EEPROM(s).

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group Memory
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**12** Command Specifier
	5	EEPROM# 00=EEPROM 1; 01=EEPROM 2
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	5	**Status** 00=Checksum Error Runtime FW, 01=OK
	6	**Major FW Revision** Binary coded
	7	**Minor FW Revision** BCD coded
	8:10	**Aux. FW Revision** Binary coded (major/minor/res.)
	11	**Major FW Revision** ASCII coded letter
	12	**Major SDRR Revision** BCD coded
	13	**Minor SDRR Revision** BCD coded
	14	**SDRR Revision Char.** ASCII coded letter
	15	**SDRR-ID** LSB binary coded
	16	**SDRR-ID** MSB binary coded
	17	**Major Booter Revision** Binary coded
	18	**Major Booter Revision** BCD coded
	19:20	*Aux. Booter Revision* Binary coded (major/minor)

F5 42 - Get HDD lightpath status (Component Status Signal Read)

This command returns information on the state of a Hard Disk Drive (HDD) slot.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**42** Command Specifier
	5	**Entity ID** (*Table 37-12* of IPMI 1.5 Spec.) of Component whose Status Signal is to be read.
	6	**Entity Instance** (0-based) of Component whose Status Signal is to be read.
	7	**Sensor Type** (*Table 36-3* of IPMISpec.) of the Sensor which reports the Status of the Component to which the Status Signal is associated.
	(8)	Option (optional) Bit 7:2 - Reserved Bit 1 :Completion Code 0x02 suppressed Bit 0 - 1 : Return ID String of Component Status Sensor
Response Data	-	**BC**
	-	**F5**
	1	**Completion Code:** 01= Status Signal not available 02 = Component not present
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	**Signal Status:** 00 = ok 01 = Identify 02 = Prefailure Warning 03 = Failure
	6	**CSS and Physical LED available:** Bit 6:0 - 0= No physical LED available Bit 6:0 > 00 = Physical LED available, Single or Multiple Color, Code Bit 7 = 0: No CSS Component Bit 7 = 1: CSS Component
	(7)	Length of ID String of Component Status Sensor (only present if Bit 0 in Request Byte 8 is set)
	(8 .. m)	Length of ID String of Component Status Sensor in ASCII chasracters (only present if Bit 0 in Request Byte 8 is set)

F5 43 - Get SEL entry long text

This command translates a given SEL entry into long text.

Request Data	-	**B8** NetFn|LUN: OEM/Group
	-	**F5** Cmd : Command Group iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**43** Command Specifier
	5:6	**Record ID** of SEL record, LS Byte first 0x0000: get first record 0xFFFF: get last record
	7	**Offset** in response SEL text
	8	**MaxResponseDataSize** size of *Converted SEL data* (16:n) in response
Response Data	-	**BC**
	-	**F5**
	1	Completion Code:
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5:6	Next Record ID
	7:8	**Actual Record ID**
	9	**Record type**
	10:13	**Timestamp**
	14	**Severity:** Bit 7: 0 = No CSS component 1 = CSS component Bit 6-4: 000 = INFORMATIONAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = Unknown’ Bit 3-0: reserved, read as 0000
	15	**Data length** of the whole text
	16:n	**Converted SEL data** requested part (n = 16 + MaxResponseDataSize - 1)
	n + 1	**String Terminator** trailing '\0' character

F5 45 - Get SEL Entry Text

This command translates a given System Event Log SEL entry into ASCII text.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**45** Command Specifier
	5:6	**Record ID** of SDR, LS Byte first
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5:6	**Next Record ID**
	7:8	**Actual Record ID**
	9	**Record type**
	10:13	**Timestamp**
	14	**Severity:** Bit 7: 0 = No CSS component 1 = CSS component Bit 6-4: 000 = INFORMATIONAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = Unknown’ Bit 3-0: reserved, read as 0000
	15	**Data length**
	16:35	**Converted SEL data**

F5 B0 - Set Identify LED

This command allows you to switch the Identify LED (blue) of the server on and off. In addition, you can set and read the GPIOs that are directly connected to the Identify LED.

You can also switch the Identify LED on and off using the Identify switch on the server.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**B0** Command Specifier
	5	**Identify LED:** 0: Identify LED off 1: Identify LED on
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first

F5 B1 - Get Identify LED

This command returns information on the status of the Identify LED (blue) of the server.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**B1** Command Specifier
Response Data	-	**BC**
	-	F5
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	5	State of Identify LED (only bit 0 is relevant)

F5 B3 - Get Error LED

This command returns information on the status of the server’s Global Error LED (red) and CSS LED (yellow). The Global Error LED indicates the most serious error status of the components. The CSS LED indicates, whether the customer himself can rpair the fault.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**B3** Command Specifier
Response Data	-	BC
	-	F5
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	5	**State of Error LED:** 0 : CSS off / GEL off 1 : CSS off / GEL on 2 : CSS off / GEL blink 3 : CSS on / GEL off 4 : CSS on / GEL on 5 : CSS on / GEL blink 6 : CSS blink / GEL off 7 : CSS blink / GEL on 8 : CSS blink / GEL blink

F5 DF - Reset Nonvolatile Cfg Variables to Default

This command forces all non-volatile IPMI settings to be set to default values.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**DF** Command Specifier
	5:8	43 4C 52 AA = ’CLR’0xaa: Security Code
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first

F5 E0 - Reset ConfigSpace variables to default

This command forces all Configuration Space variables to be set to default values.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**E0** Command Specifier
	5:8	43 4C 52 AA = ’CLR’0xaa: Security Code
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first

F5 F8 - Delete User ID

The system supports up to 16 users. This command allows individual iRMC S2/S3 users to be deleted.

CAUTION!

The system can no longer be managed if all iRMC S2/S3 users are deleted.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS byte first
	4	**F8** Command Specifier
	5:8	User ID (1-16)
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS byte first

12.2 Configuring the iRMC S2/S3 via SCCI and scripted configuration

This section provides information on the following topics:

- How to use an SCCI (**S**erverView **C**ommon **C**ommand **I**nterface) compliant interface for configuring the iRMC S2/S3.
- Scripted configuration of the iRMC S2/S3

12.2.1 iRMC S2/S3 configuration data

Please note that the interface described below is mainly for remote configuration and is **not** an SCCI implementation. It only uses the SCCI command and configuration definitions and the SCCI file format.

12.2.1.1 Overview

The iRMC S2/S3 stores internal configuration data in two separate sections of its NVRAM (Non-volatile RAM):

- FTS-specific ConfigSpace data, which is addressed by the firmware via a fixed internal description table.
- Original, manufacturer-specific NVCFG data, which is accessed by offset definitions.

Some configuration data from the original NVCFG data is internally mapped by the firmware to be accessible via ConfigSpace access methods. For instance, DNS servers and DNS configuration of the iRMC S2/S3 can be accessed both via IPMI OEM LAN configuration parameters and via ConfigSpace. Both methods access the same low level data structures in the original NVCFG area.

Non-iRMC S2/S3-specific ServerView software components (e.g. the ServerView Agents or the Server Configuration Manager) in some cases also map standard IPMI related commands and configuration items, such as standard IPMI user configuration or IPv4 network configuration. This implements an abstraction level between the IPMI BMC layer and higher software levels.

The SCCI is a generic application programming interface (API) defined by Fujitsu for different Server Management Controller hardware as well as Server Management software (e.g. ServerView Agents). It can be easily extended to cover new commands or new configuration items. For an architectural overview of the SCCI, see the online help of the ServerView agents.

Starting with iRMC S2 firmware 5.20A (IPv6 version), the iRMC S2/S3 supports remote configuration and limited scripting via the */config URL* in the iRMC S2/S3.

Benefits of remote iRMC S2/S3 configuration via web-based access

Remote configuration of the iRMC S2/S3 via web-based access provides the following benefits:

- Uses HTTP POST operation for uploading files onto the iRMC S2/S3. No special tool is required. Any generic tool or scripting environments supporting authenticated HTTP POST operations can be used. Sample scripts can be found on the ServerView Suite DVD 1.
- Uses built-in authentication and authorization methods of the iRMC S2/S3 Web server.
- Supports HTTP 1.1 Basic and Digest authentication based on RFC 2617 with local iRMC S2/S3 user accounts.
- Features optional built-in strong encryption with standard HTTPS-based access.
- Can be used with global user accounts (managed by an LDAP directory service) and HTTP 1.1 Basic authentication.

  i If HTTP 1.1 Basic authentication is used, it is recommended that, for encryption and confidentiality reasons, you use the HTTPS protocol to protect the username/password combination.
- Uses a configuration file format that is based on XML. You have the option to edit the file manually, or to export it from a reference installation or from the Server Configuration Manager.

  The configuration file can be re-used with other SCCI based installation methods (e.g. Server Configuration Manager).
- Can be easily extended to new configuration items and new supported SCCI commands.

12.2.1.2 SCCI file format

i The format of the XML configuration file (*.pre*) used is taken from the setup configuration help file that is installed together with the ServerView agents on Windows platforms. A copy of this description with iRMC S2/S3-specific notes is shown below.

The configuration file is a based on XML syntax:

- Each configuration setting consists of a simple XML fragment starting with a "`<CMD>`" tag.
- The complete sequence of configuration settings is enclosed in a pair of tags "`<CMDSEQ>` and `</CMDSEQ>`".

The following is an example of a typical command sequence comprising two configuration settings:

```
<CMDSEQ>
<CMD Context="SCCI" OC="ConfigSpace" OE="3800" OI="0"
Type="SET">
<DATA Type="xsd::hexBinary" Len="1">04</DATA>
<CMD Context="SCCI" OC="ConfigSpace" OE="3801" OI="0"
Type="SET">
<DATA Type="xsd::hexBinary" Len="1">00</DATA> </CMD>
</CMDSEQ>
```

The *Context* parameter is used internally to select the provider of the operation. Currently, `SCCI` is the only supported provider.

Parameters of SCCI provider-specific commands

The following SCCI-provider-specific commands are available:

Operation Code (`OC`)

Hex value or string specifying the command / operation code.

> The iRMC S2/S3 only supports a limited set of SCCI commands. For a list of supported commands see table "SCCI commands supported by the iRMC S2/S3" on page 420

Operation Code Extension (`OE`)

Hex value for extended operation code. Default: `OE=0`

For ConfigSpace Read-/Write operations, this value defines the ConfigSpace ID.

Object Index (`OI`)

Hex value selecting an instance of an object. Default:OI=0"

Operation Code Type (`Type`)

For configuration settings, the values `GET` (read operation) and `SET` (write operation) are supported. Default: Type=GET

> `SET` operations require data. For specifying the appropriate data type, use the *Data (DATA)* parameter described below.

Cabinet Identifier (`CA`)

Allows you to select an extension cabinet and use its cabinet ID number.

> Do **not** use this parameter to request for the system cabinet!

Data (`DATA`)

If a `SET` parameter (write operation) is specified: Data type (`Type` parameter), and, in some cases, data length (`LEN` parameter) are required.

Currently, the following data types are supported:

– `xsd::integer`

Integer value

Example

```
<DATA Type="xsd::integer">1234</DATA>
```

- `xsd::hexBinary`

  Stream of bytes. Each byte is coded in two ASCII characters. Use the `Len` parameter as shown in the example below to specify the length of the stream (i.e. the number of bytes).

  The data type `xsd::hexBinary` can be used without any restriction.

  Example

  A stream of four bytes `0x00 0x01 0x02 0x04` will be coded as the following ASCII stream:

  ```
  <DATA Type="xsd::hexBinary" Len="4">0001020304</DATA>
  ```

- `xsd::string`

  Normally used for the transfer of strings. Additionally, the `string` type can be used for IPv4 addresses and MD5-based user passwords. In this case, the string data is internally converted to the accepted target format.

  Transferring encrypted data

  A Fujitsu-proprietary data encryption is supported for some sensitive data such as user or service (LDAP/SMTP) access passwords, or the AVR license key of the iRMC S2/S3. You can use the *iRMC_PWD.exe* program for encrypting password data (see section "Generating encrypted passwords with iRMC_PWD.exe" on page 424).

  `Encrypted="1"` must be set in the `<DATA>` tag to indicate that the data to be written is encrypted.

  Examples

  Transferring the string "Hello World":

  ```
  <DATA Type="xsd::string">Hello World</DATA>
  ```

  Transferring a password as clear (readable) text:

  ```
  <DATA Type="xsd::string">My Readable Password</DATA>
  ```

  Transferring an encrypted password:

  ```
  <DATA Type="xsd::string"
  Encrypted="1">TpVlTJwCyHEIsC8tk24ci83JuR9l</DATA>
  ```

Transferring the IPv4 address "192.23.2.4"

```
<DATA Type="xsd::string">192.23.2.4</DATA>
```

CAUTION!

The `xsd::string` data type is restricted to readable strings, IP addresses and MD5-based user passwords.

For all other data, the `xsd::hexbinary` data type must be used!

Do not directly specify the characters ä, ö, ü, etc. in strings unless they are actually needed by the using application!

Both SCCI and the ConfigSpace interface do not store any character encoding information. Thus, any non-US-ASCII-characters will be interpreted internally by the using application and therefore should be avoided.

If you do actually need to specify special characters, make sure that you edit and save your file in UTF-8 format including the correct BOM.

Command Status (`Status`)

After the configuration settings are transferred, the `Status` contains the result of the operation. If the operation has completed successfully, the value `0` is returned.

For a specification of all public configuration settings (ConfigSpace) see the *SCCI_CS.pdf* file, which you will find in the *Help* folder of the ServerView Agents installation package. Additionally, the *SCCI_CS.pdf* file is distributed with the PRIMERGY Scripting Toolkit.I

12.2.1.3 Restrictions

All commands specified in the *.pre* file are normally executed sequentially. The following are exemptions from this rule:

- To prevent broken network connectivity, commands for IPv4 and VLAN network configuration are executed at the end of a command sequence.
- Currently, IPv6 configuration is limited to the configuration of the non-volatile IPv6 configuration parameters.

  As a workaround, you can proceed as follows:

  1. Arrange your script as follows:

     a) At the beginning of the script: Disable IPv6.

     b) Configure IPv6 parameters.

     c) At the end of the script: Enable IPv6

  2. Submit the script from an IPv4 address.
- The SSL certificate and the related matching private key are executed at the end of a command sequence. Both components must be present in the same *.pre* file and are checked for matching each other.
- If a power management operation for the managed server or a reboot of the iRMC S2/S3 is required or desired:

  It is recommended (but not required) to run these commands in separate command files. You can achieve this e.g. by splitting the configuration and power management operations into separate tasks.
- Optional time delays between the execution of consecutive commands must implemented outside the script.

  For example, you can achieve this as follows:

  1. Devide the script appropriately into separate scripts.
  2. Use the functional range of the client to insert time delays between sending the individual files.

12.2.1.4 Exporting / importing configuration data from / on the iRMC S2/S3

The *Save iRMC S2/S3 Firmware Settings* page of the iRMC S2/S3 web interface allows you to save (export) the current iRMC S2/S3 configuration data in a configuration file (*.pre*). As well, you can import iRMC S2/S3 configuration data from an existing configuration file (*.pre*), i.e. load configuration data onto the iRMC S2/S3 (for details, see section "Save iRMC S2/S3 Firmware Settings - Save firmware settings" on page 169.)

To import an iRMC S2/S3 configuration, you can alternatively send the corresponding SCCI command file to the */config URI* of the iRMC S2/S3 via the HTTP POST operation.

12.2.2 Scripted configuration of the iRMC S2/S3

This section describes provides information on the following topics:

- SCCI commands supported by the iRMC S2/S3.
- Using various script languages for scripted configuration of the iRMC S2/S3.
- Generating encrypted passwords with the *iRMC_PWD.exe* program.

12.2.2.1 List of SCCI commands supported by the iRMC S2/S3

The SCCI commands supported by the iRMC S2/S3 are shown in table 19:

SCCI OpCode	SCCI Command String	Description
0xE002	ConfigSpace	ConfigSpace Write
0x0111	PowerOnCabinet	Power On the Server
0x0112	PowerOffCabinet	Power Off the Server
0x0113	PowerOffOnCabinet	Power Cycle the Server
0x0204	ResetServer	Hard Reset the Server
0x020C	RaiseNMI	Pulse the NMI (Non Maskable Interrupt)
0x0205	RequestShutdownAndOff	Graceful Shutdown, requires running Agent
0x0206	RequestShutdownAndReset	Graceful Reboot, requires running Agent
0x0209	ShutdownRequestCancelled	Cancel a Shutdown Request
0x0203	ResetFirmware	Perform a BMC Reset
0x0250	ConnectRemoteStorageServer	Connect or Disconnect a standalone Remote Storage Server

Table 19: SCCI commands supported by the iRMC S2/S3

12.2.2.2 Scripting with cURL

The open source command-line tool cURL allows you to transfer data specified with URL syntax. You can download the latest version of the source code as well as precompiled versions for different operating systems from *http://curl.haxx.se/*.

The following are some examples of how to use curl to send a configuration file to the iRMC S2/S3.

For details on the curl command line options please refer to the curl documentation.

- HTTP Access with Basic Authentication (default) and the default iRMC S2/S3 admin account:

  ```
  curl --basic -u admin:admin --data @Config.pre
  http://<iRMC S2/S3 IP address>/config
  ```

- HTTP Access with Digest Authentication and the default iRMC admin account

  ```
  curl --digest -u admin:admin --data @Config.pre
  http://<iRMC S2/S3 IP address>/config
  ```

- HTTPS Access with no certificate check (-k) and Digest authentication and the default iRMC admin account:

  ```
  curl --digest -k -u admin:admin --data @Config.pre
  https://<iRMC S2/S3 IP address>/config
  ```

- HTTPS Access with an LDAP user account.

  Please note, that for LDAP users you have to specify Basic authentication

  ```
  curl --basic -k -u LDAPuser:LDAPpassword --data @Config.pre
  https://<iRMC S2/S3 IP address>/config
  ```

12.2.2.3 Scripting with Visual Basic (VB) Script

The following VB script sends a configuration file to the iRMC S2/S3:

```
IP_ADDRESS = "<iRMC S2/S3 IP address>"
USER_NAME  = "admin"
PASSWORD   = "admin"

FILE_NAME  = ".\\ConfigFile.pre"

Const ForReading = 1
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.OpenTextFile(FILE_NAME, ForReading)
' --------------------------------------------------------------
On Error Resume Next

Set xmlHttp = CreateObject("Microsoft.XMLHTTP")
xmlHttp.Open "POST", "http://" & IP_ADDRESS & "/config", False,
USER_NAME, PASSWORD
xmlhttp.setRequestHeader "Content-Type", "application/x-www-
form-urlencoded"
xmlHttp.Send objFile.ReadAll

Wscript.Echo xmlhttp.responsexml.xml
```

12.2.2.4 Scripting with Python

```
#!/usr/bin/python3
import sys
import httplib2
from urllib.parse import urlencode

# ==============================================================
# iRMC

USER = 'admin'
PWD  = 'admin'
IP_ADDR =  '192.168.1.100'
# ==============================================================

h = httplib2.Http()

# Basic/Digest authentication
h.add_credentials(USER, PWD)

def doit(data,ausgabe=sys.stdout):
  try:
    resp, content = h.request("http://%s/config" % IP_ADDR,
    "POST", data)
    if resp['status'] == '200'
      data = content.decode('utf-8')
      print(data,file=ausgabe)
      else:
      print('STATUS:',resp['status'],file=ausgabe)
      print(str(resp),file=ausgabe)
  except Exception as err:
    print('ERROR:',str(err),file=ausgabe)
  print()


# Example 1 - send a configuration file to the iRMC S2/S3
try:
  data = open('ConfigFile.pre').read()
  doit(data)
except Exception as err:
  print('ERROR:',str(err),file=ausgabe)


# Example 2 - Set Config Space Values
# 0x200 (ConfCabinetLocation) and
# 0x204 (ConfSystemContact) direct from the script
#
LocationContact = '''<?xml version="1.0" encoding="UTF-8"
standalone="yes" ?>
```

```
<CMDSEQ>
  <!-- ConfCabinetLocation -->
  <CMD Context="SCCI" OC="ConfigSpace" OE="200" OI="0" >
    <DATA Type="xsd::string">%s</DATA>
  </CMD>
  <!-- ConfSystemContact -->
  <CMD Context="SCCI" OC="ConfigSpace" OE="204" OI="0" >
    <DATA Type="xsd::string">%s</DATA>
  </CMD>
</CMDSEQ>
'''

doit(LocationContact % ("Ostsee","Kiel"))
```

12.2.2.5 Generating encrypted passwords with iRMC_PWD.exe

The Fujitsu Technology Solutions iRMC password encryption and verification Utility *iRMC_PWD.exe* is a Win32 program allowing you to generate encrypted passwords for use with SCCI scripting. *iRMC_PWD.exe* can be used both to encrypt a single password and to generate a SCCI batch file for scripted configuration.

iRMC_PWD standard command line options

[-h] [-?]
: This help.

[-v]
: Verify an encrypted password string.

[-o] <oid>
: The Object ID for the data to be encrypted.

[-u] <username>
: Username for the given Object ID (optional).

[-p] <password>
: Password for the given Object ID / / encrypted password string to be verified.

[-x] <opCodeExt>
: Opcode extension for the ConfigSpace data to encrypt.

[-p] <password>
Password for the given Object ID.
Default:1452 (ConfBMCAcctUserPassword)

Supported values:

1273 - ConfAlarmEmailSMTPAuthPassword

[-p] <password>
Password for the given Object ID.
Default: 1452 (ConfBMCAcctUserPassword)

Supported Values:

1452 - ConfBMCAcctUserPassword

1273 - ConfAlarmEmailSMTPAuthPassword

197A - ConfLdapiRMCgroupsUserPasswd

1980 - ConfBMCLicenseKey

iRMC_PWD command line output options

[-b]
Creates the output file as a WinSCU BATCH file.

[-f] <Output File>
Specify the output file name.
Default: *iRMC_pwd.txt*
Default in Batch mode: *iRMC_pwd.pre*

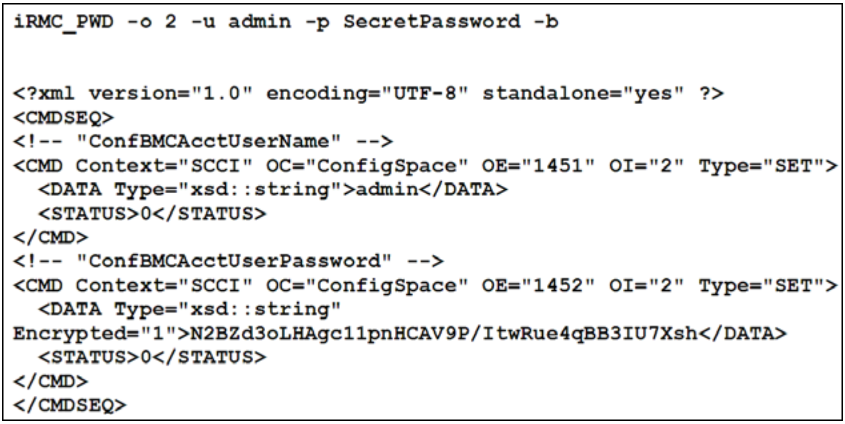
Example

You want to generate a *.pre* file that sets/changes the username to `admin` and the password to `SecretPassword` for the (existing) user with the oid `2`.

To achieve this, enter the following command:

```
iRMC_PWD -o 2 -u admin -p SecretPassword -b
```

iRMC_PWD will generate a *.pre* file with the contents shown in figure 226 on page 426.



```
iRMC_PWD -o 2 -u admin -p SecretPassword -b


<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<CMDSEQ>
<!-- "ConfBMCAcctUserName" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1451" OI="2" Type="SET">
  <DATA Type="xsd::string">admin</DATA>
  <STATUS>0</STATUS>
</CMD>
<!-- "ConfBMCAcctUserPassword" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1452" OI="2" Type="SET">
  <DATA Type="xsd::string"
Encrypted="1">N2BZd3oLHAgc11pnHCAV9P/ItwRue4qBB3IU7Xsh</DATA>
  <STATUS>0</STATUS>
</CMD>
</CMDSEQ>
```

Figure 226: Contents of the generated .pre file